CAPÍTULO SEGUNDO

LAS PREMISAS TECNOLÓGICAS DE LA INNOVACIÓN EN EL ÁMBITO DE LAS ADMINISTRACIONES PÚBLICAS. IMPLICACIONES Y DESAFÍOS DESDE LA PERSPECTIVA JURÍDICA

ÍNDICE

I. La necesaria redefinición de las relaciones entre Derecho y tecnología en el contexto de la Administración electrónica 139

II. Principales herramientas tecnológicas en la Administración electrónica: análisis jurídico desde la perspectiva de la innovación 148

1. La firma electrónica 148

a) La firma electrónica, un concepto jurídico anfibológico 148

b) La distinta eficacia de los tipos de firma electrónica y su proyección sobre los documentos electrónicos de las Administraciones Públicas 154

c) Las singularidades de la regulación de la firma electrónica en el ámbito de las Administraciones Públicas 160

d) Las comprobaciones relativas al uso de la firma electrónica en la gestión documental: problemas y disfunciones derivados de la intermediación de prestadores de servicios de certificación 167

e) Implicaciones jurídicas de los desajustes en la regulación de la firma electrónica como consecuencia de su singularidad tecnológica 173

2. La relevancia jurídica de las exigencias de seguridad e interoperabilidad en la Administración electrónica 179

a) El Esquema Nacional de Seguridad 182

b) Las condiciones de interoperabilidad y el ENI 186

III. Entre el cumplimiento del Derecho y el potencial innovador de la Administración electrónica: perspectiva jurídica de un difícil equilibrio . . 192

1. La necesaria reconfiguración de los conceptos jurídicos al trasluz de las singularidades tecnológicas . . 192

2. Consecuencias jurídicas del incumplimiento de las garantías tecnológicas 198

I. LA NECESARIA REDEFINICIÓN DE LAS RELACIONES ENTRE DERECHO Y TECNOLOGÍA EN EL CONTEXTO DE LA ADMINISTRACIÓN ELECTRÓNICA

Las tecnologías de la información y la comunicación suponen un relevante desafío para la efectividad de las normas jurídicas que regulan la actividad de las Administraciones Públicas y sus relaciones con los ciudadanos. En efecto, si bien es indudable que su uso constituye una exigencia de eficacia y, sobre todo, de adaptación al entorno social y económico en que han de llevar a cabo sus funciones, lo cierto es que al amparo de tal justificación puede pasar desapercibido –o, en algunos casos, minusvalorado– el riesgo que existe de otorgar un papel secundario al destacado protagonismo que, sin embargo, ha de jugar el Derecho en el proceso de modernización tecnológica en el ámbito administrativo[87]. Resulta, por tanto, imprescindible no ya advertir acerca de esta problemática sino, más bien, analizar las razones por las cuales se genera dicha situación y, en particular, ofrecer cri-

[87] En palabras de Piñar, «no basta con subrayar sólo el hecho de que las Administraciones Públicas deben modernizarse al son de los avances tecnológicos, y adaptar en consecuencia su organización y procedimientos a la nueva y siempre mutable realidad, sino de proponer la necesidad de reconsiderar el concepto mismo de Derecho y Administración» (J. L. Piñar Mañas, «Revolución tecnológica…», ob. cit., p. 26).

terios interpretativos para impedir o, al menos, minimizar sus nefastas consecuencias.

Por lo que se refiere a estas últimas, se trata en definitiva de garantizar la superioridad del Derecho frente a los criterios, reglas y normas tecnológicos, de manera que no resulten socavados los cimientos del Estado de Derecho. En concreto, puede darse el caso de que las normas jurídicas se encuentren desfasadas o sean inadecuadas, de manera que se conviertan en una barrera a la hora de implantar proyectos de Administración electrónica, facilitándose por tanto la tentación de desplazar su aplicación dadas las ventajas que ofrece la tecnología. Asimismo, cabe imaginar que las garantías jurídicas, en lugar de cumplir su esencial papel como reglas del juego que aseguran el respeto de los diversos intereses públicos y privados afectados, se perciban como un inconveniente que dificulta alcanzar el potencial que permitirían los programas y equipos informáticos de obviarse su aplicación; por lo que la tensión entre Derecho y tecnología puede romperse a favor de esta última con relativa facilidad a menos que se advierta claramente de las consecuencias que dicho resultado podría conllevar y, sobre todo, se establezcan las medidas que impidan este indeseable resultado.

En el fondo de este problema se encuentra muchas veces el excesivo papel protagonista que ha correspondido al personal con perfil técnico en el diseño e impulso de los proyectos institucionales relacionados con la Administración electrónica[88]. Ciertamente, se trata de una inercia más

[88] Un reciente pero significativo episodio es la Resolución de la Secretaría de Estado de Administraciones Públicas por la que se aprueba la norma técnica de interoperabilidad de política de gestión de documentos electrónicos (BOE n. 178, 26 julio, 2012), cuyo objeto trasciende claramente el ámbito

acentuada en los primeros momentos y que progresivamente está llamada de diluirse, pero que en gran medida se explica por la singularidad del conocimiento técnico requerido, del que han carecido tradicionalmente la mayor parte de los empleados públicos, en particular los encargados de funciones directivas en servicios comunes. En consecuencia, han sido los servicios informáticos de las respectivas instituciones los que han impulsado o, al menos, supervisado los proyectos de modernización tecnológica, superando su ámbito material propio ante la falta de preparación y, en ocasiones, de interés por parte de quien estaba llamado a liderar este tipo de iniciativas.

Desde una estricta consideración institucional y, al margen de las excepciones que hayan podido darse, lo cierto es que los servicios jurídicos de las Administraciones Públicas tampoco han jugado el papel que les debería corresponder en relación con la modernización tecnológica. De este modo, con relativa frecuencia ni siquiera han tenido noticia de los desarrollos y aplicaciones informáticas que se estaban implementando en su propia entidad o, de haberles informado, en general se ha adoptado una actitud pasiva cuando no obstruccionista; postura que, en última instancia, se encontraba motivada tanto por la falta de cualificación básica –en el sentido de mínima o elemental– en relación con el funcionamiento de las tecnologías empleadas como, en muchos casos y sin que sean razones incompatibles sino incluso complementarias, por una inadmisible actitud defensiva y de autoprotección ante los problemas que eventualmente

estricto de la interoperabilidad para establecer criterios generales de gestión documental.

pudieran darse en el futuro por lo que se refiere al normal funcionamiento de los servicios.

La falta de compromiso que, incluso hoy día, se observa en la formación de juristas en el ámbito universitario en relación con las implicaciones de las tecnologías de la información y la comunicación no ayuda, precisamente, a solventar esta deficiencia. No se trata ya tanto de que, salvo relevantes excepciones y al margen de las actividades de postgrado, las asignaturas dedicadas específicamente a las implicaciones jurídicas de la tecnología hayan brillado por su ausencia sino, incluso y más que nada, de que en la mayor parte de las materias generales –Derecho Administrativo, Civil, Procesal…– ni siquiera se hace la más mínima referencia al impacto que la tecnología está teniendo en la reconfiguración de las categorías tradicionales y, como veremos más adelante, de las garantías jurídicas en las que se han venido sustentando hasta ahora la protección de los diversos intereses tutelados por las normas.

Sin embargo, una sociedad en gran medida dependiente de la tecnología como la actual ha de afrontar importantes retos de diversa índole, entre los que destacan a los efectos que ahora interesan los de carácter jurídico y, en particular, jurídico-administrativos. De lo contrario existe un riesgo cierto de que el principio constitucional de sometimiento del Estado al Derecho –y, en concreto, de la Administración Pública– subsista simplemente sobre el papel por su reconocimiento formal en la Norma Fundamental pero desprovisto, sin embargo, de efectividad material. Se trata de un desafío que ha de plantearse tanto por lo que respecta a la supremacía de la norma jurídica respecto de los criterios fijados por quien haya programado las aplicaciones, en relación con el

efectivo respeto al ejercicio competencial por parte de los titulares de los órganos administrativos que, en principio, son quienes han de adoptar las decisiones que vinculan a las Administraciones Públicas; como, en última instancia, por lo que se refiere a la capacidad de control por parte de jueces y magistrados que, dada la complejidad tecnológica inherente a los servicios, quedará en gran medida en manos de informes periciales. ¿Cuáles son pues las principales razones que justifican la magnitud de este desafío?

Como se ha destacado certeramente[89], resulta ingenuo pretender un control absoluto de la tecnología por parte del Derecho, esto es, en relación a cada uno de los detalles y aspectos menores del funcionamiento de las aplicaciones informáticas y los sistemas de información. Así pues, hemos de partir de esta premisa a la hora de realizar el análisis que nos ocupa, distinguiendo a estos efectos cuáles han de considerarse exigencias esenciales para asegurar sustancialmente la primacía del Derecho sobre la tecnología, en particular por lo que respecta a aquellas contradicciones especialmente destacadas que, por tanto, debieran dar lugar a consecuencias invalidantes de la actuación administrativa. Para ello, han de identificarse previamente aquellos peligros sustanciales derivados de la singularidad tecnológica en que se sustenta la Administración electrónica pues, de lo contrario, difícilmente cabría afrontar la delicada tarea de determinar las implicaciones jurídicas de las contradicciones con las normas que resulten de aplicación.

En primer lugar, en relación con las aplicaciones informáticas existe una tendencia a la utilización de normas téc-

[89] J. Esteve Pardo, *Técnica*..., ob. cit., p. 27.

nicas y certificaciones de proyección internacional a través de las cuales garantizar, al menos, unas mínimas exigencias a partir de la normalización de la calidad y seguridad. No obstante, muchas de estas normas se basan en estándares técnicos que, sin embargo, no implican necesariamente su respeto a las normas jurídicas aplicables en el ámbito interno de los Estados y, asimismo, de cada una de las Administraciones Públicas; esto es, no siempre tienen en cuenta las singularidades propias del respectivo sistema jurídico-administrativo, característica especialmente reforzada en el caso de estructuras descentralizadas como la española. En consecuencia, a la hora de que aquéllas contraten con terceros el desarrollo o, en su caso, la adquisición de aplicaciones para prestar servicios electrónicos, han de fijar claramente que, al menos desde el punto de vista jurídico, los estándares tecnológicos han de supeditarse necesariamente al cumplimiento de las normas jurídicas que resulten de aplicación en función del servicio de que se trate, tal y como puede suceder singularmente con los registros electrónicos, los gestores documentales o las plataformas de contratación. Sobre todo si tenemos en cuenta que, como destacaremos más adelante, la tendencia actual a la externalización se está materializando a través del denominado *cloud computing* que, al menos con carácter general, puede suponer la gestión de servicios y el manejo de información a través de equipos informáticos pertenecientes a empresas ubicadas en otro Estado.

Por otra parte, la complejidad añadida que caracteriza sobre todo el funcionamiento de ciertas aplicaciones determina que, en ocasiones, la creciente externalización propia de este ámbito ni siquiera pueda ser supervisada por el personal al servicio de la Administración Pública, tanto desde

el punto de vista técnico como jurídico. Es más, resulta frecuente que en las condiciones de uso de tales aplicaciones se establezcan cláusulas que impidan indirectamente que dicho control se lleve a cabo, de manera que ni la propia entidad pública contratante puede constatar el efectivo respeto al marco jurídico aplicable. Al margen, claro está, de aquellos supuestos en que, aun cuando tal posibilidad no se encuentra impedida contractualmente, el personal propio carece del conocimiento necesario para fijar las condiciones técnicas que han de respetar las aplicaciones o, simplemente, supervisar su funcionamiento y, en consecuencia, el cumplimiento por parte del contratista de las condiciones técnicas previstas en los pliegos.

Más aún, el uso de medios electrónicos en la gestión administrativa permite llevar a cabo tratamientos más intensivos de información, tanto desde una estricta consideración cuantitativa como, sobre todo, cualitativa. En consecuencia, tal y como se ha destacado anteriormente, debe tenerse en cuenta que las normas tradicionales actualmente en vigor en materia de protección de datos personales se encuentran desfasadas, hasta el punto de que cabe poner en duda que la simple aplicación de los principios generales en la materia resulten suficientes para asegurar una adecuada protección jurídica; al menos si tenemos en cuenta la práctica que, en general, se ha venido llevando a cabo en el ámbito de la Administración electrónica, con manifiesto menosprecio en muchos casos de las exigencias legales en relación con el principio de finalidad –artículo 4 LOPD, que prohíbe los usos incompatibles con aquéllos que justificaron la recogida de la información–, las medidas de seguridad –artículo 9 LOPD–, el deber de información –artículo 5 LOPD– o,

sin ánimo exhaustivo, el principio de proporcionalidad en la difusión de la información –artículo 4 LOPD–.

Antes al contrario, dado el mayor peligro potencial que supone el uso de la informática para las libertades de los ciudadanos, debería reforzarse la exigencia en el cumplimiento estricto de las reglas vigentes, incluso desde la perspectiva estrictamente formal y del cumplimiento de las obligaciones de esta naturaleza, sin que resulte admisible una injustificada flexibilidad amparada en una supuesta eficacia que postergue las garantías jurídicas. En este sentido, es necesario reiterar la necesidad de llevar a cabo un replanteamiento del alcance de las consecuencias del incumplimiento de estas normas[90], sobre todo si tenemos en cuenta que se trata de una garantía fijada en la Norma Fundamental que, en última instancia, podría ser extendida más allá del limitado alcance que el Tribunal Constitucional ha otorgado al artículo 18.4, circunscrito hasta ahora a la protección de las personas físicas frente al uso indebido de sus datos personales.

Una reflexión final debe realizarse desde la perspectiva material. En concreto, es necesario recordar que el uso de medios electrónicos puede suponer un reforzamiento de las garantías jurídicas siempre que efectivamente se utilicen las posibilidades que permite la tecnología para impedir la alteración de los documentos y acreditar las circunstancias

---

[90] Hasta ahora las aportaciones han sido ciertamente limitadas y en gran medida sólo constituyen una primera aproximación, debiendo destacarse el intento de A. Palomar Olmeda, *La actividad…*, ob. cit., pp. 268 y ss.; y, desde la perspectiva del régimen jurídico de la protección de los datos de carácter personal, J. Valero Torrijos, «La invalidez de los actos administrativos dictados en base a datos personales contenidos en ficheros irregulares», en M. A. Davara (coord.), *XIV Encuentros sobre Informática y Derecho 2000-2001*, Arazandi, Pamplona, 2001, pp. 193 a 204.

temporales en que se generan o, por lo que respecta a los accesos a la información, restringirlos exclusivamente a las personas o sistemas que requieran conocer de tales datos en razón de las funciones asignadas. Ahora bien, precisamente debido a las facilidades que permite la tecnología, si no se refuerza el efectivo cumplimiento –y, sobre todo, su exigencia– de las normas técnicas que aseguren tales extremos, lo cierto es que puede darse una cierta apariencia de garantía y cumplimiento que, sin embargo, no obedezca a la realidad; de manera que las medidas técnicas limiten su virtualidad simplemente al plano teórico y, por tanto, en la práctica queden sin asegurarse cuestiones tan esenciales y, al mismo tiempo, elementales como la integridad y autenticidad de los documentos, las limitaciones en el acceso a la información personal y, en caso de contravención, las condiciones fácticas en que ha tenido lugar la infracción o, sin ánimo exhaustivo, la constancia de las comunicaciones realizadas y la prueba de las circunstancias en que las mismas se han producido, tanto a nivel interno como por lo que respecta a las que tengan lugar con los ciudadanos u otras entidades.

II. PRINCIPALES HERRAMIENTAS TECNOLÓGICAS EN LA ADMINISTRACIÓN ELECTRÓNICA: ANÁLISIS JURÍDICO DESDE LA PERSPECTIVA DE LA INNOVACIÓN

1. LA FIRMA ELECTRÓNICA

a) La firma electrónica, un concepto jurídico anfibológico

La utilización de la firma manuscrita como garantía de la integridad y la autenticidad de los documentos se ha consolidado tradicionalmente como la principal medida por lo que respecta al soporte papel, mientras que la confidencialidad en las comunicaciones se ha sustentado en la entrega personal de los documentos a los destinatarios mediante sobres cerrados. Sobre este doble paradigma ha venido funcionado la gestión administrativa y las comunicaciones con los ciudadanos, si bien la informática ha conllevado el cuestionamiento de tales premisas ante la dificultad o, incluso, inviabilidad de aplicarlas en los nuevos soportes electrónicos y en las redes telemáticas. Mientras que las tradicionales e insuficientes garantías de intangibilidad que ofrecen a este respecto los documentos escritos y la firma manuscrita no resultan de aplicación a los documentos y relaciones que se establecen a través de las modernas herramientas tecnológicas, y en especial a través de una red abierta como Internet, existen en la actualidad dispositivos técnicos que permiten asegurar con mayores dosis de fiabilidad las exigencias de identificación e integridad antes referidas, destacando entre todas ellas por su seguridad la firma electrónica.

Sin embargo, no todas las modalidades de firma electrónica ofrecen idénticos niveles de seguridad a los efectos de cumplir los requerimientos técnicos a los que se acaba de aludir; de manera que las exigencias antes referidas sólo se cumplirán en su grado máximo –al menos actualmente– a través de una concreta modalidad de firma electrónica, la denominada *firma digital*, que, al estar basada en el uso de sistemas criptográficos, permite garantizar que el remitente no ha sido suplantado y que el documento y, en general, la información no han sido modificados[91]. Se trata, por tanto, de una distinción cuyas consecuencias jurídicas son de gran relevancia, de ahí que dediquemos una especial atención a precisar la eficacia que presentan cada una de estas modalidades a partir de la regulación legal. Nos encontramos, pues, ante un requisito de carácter técnico legalmente exigido, como analizaremos más adelante para los documentos administrativos electrónicos, que, en función de la modalidad a la que se refiera, tendrá una eficacia u otra por lo que respecta a la identificación del firmante[92] y la integridad

---

[91] A. Martínez Nadal, *Comentarios a la Ley de Firma electrónica*, 2ª ed., Thomson-Reuters, Madrid, 2009, p. 81.

[92] En todo caso, como señala con acierto A. Rodríguez Adrados (*La seguridad de la firma electrónica. Consecuencias de su uso por un tercero*, Consejo General del Notariado, Madrid, 2005, pp. 22 y ss.), en puridad la firma electrónica sólo identifica al solicitante/titular de los certificados y no a quien realmente la utiliza, de ahí que se refiera a la firma electrónica como un *sello* más que como una firma. Específicamente, por lo que se refiere a las Administraciones Públicas, cfr. F. Bauzà Martorell, *Procedimiento administrativo electrónico*, Comares, Granada, 2003, pp. 65 a 76. En relación con la actividad probatoria relacionada con la firma electrónica, a estos efectos véase I. Alamillo Domingo y X. Uríos Aparisi, «Comentario crítico a la Ley 59/2003, de 19 de diciembre, de Firma Electrónica», *Revista de Contratación Electrónica*, núm. 46, 2004, pp. 59 a 63.

de la información, es decir, del documento administrativo en cuestión[93]. En efecto, el legislador español –siguiendo a estos efectos el modelo comunitario[94]– ha partido de un concepto amplio de firma electrónica que, en consecuencia, nos obliga a precisar el alcance de su utilización en cada caso concreto; en particular por lo que se refiere al ámbito de las Administraciones Públicas si tenemos en cuenta que la regulación legal básica sobre acceso de los ciudadanos a los servicios públicos electrónicos, lejos de establecer una disciplina rígida y cerrada, ha optado por un modelo flexible basado en el expreso reconocimiento de varias modalidades de firma electrónica y la fijación –artículo 4.g) LAE– de un principio general de proporcionalidad por lo que se refiere a las medidas de seguridad técnicas, en virtud del cual sólo se exigirán aquellas que «sean adecuadas a la naturaleza y circunstancias de los distintos trámites y actuaciones»[95].

---

[93] En opinión de A. Palomar Olmeda «corresponde al titular de la competencia administrativa acreditar su titularidad y la de la de los medios instrumentales utilizados para exteriorizar sus manifestaciones de voluntad [...]», de manera que si niega «haber realizado una determinada manifestación tendrá que probar la diligencia en la custodia de las claves, su denuncia ante las autoridades si se ha percatado de su utilización ilegal y, en general, mostrar una actitud que permita entender deshecha la presunción de que la actuación ligada a la firma electrónica corresponde al titular» (*La actividad administrativa efectuada por medios electrónicos*, Thomson-Aranzadi, Cizur Menor, 2007, p. 287).

[94] Artículo 2 de la Directiva 1999/93/CE del Parlamento Europeo y del Consejo, de 13 de diciembre de 1999, por la que se establece un marco comunitario para la firma electrónica.

[95] Así pues, según advierte I. Martín Delgado, debe existir una relación directa entre los datos que se manejen en el trámite y el nivel de seguridad que requieran los intereses afectados por el mismo [«Identificación y autenticación de los ciudadanos», en E. Gamero Casado y J. Valero Torrijos (coords.), *La Ley de Administración electrónica. Comentario sistemático a la Ley 11/2007, de*

El concepto de firma electrónica utilizado por el legislador español se basa en la regulación europea que ofrece la Directiva 1999/93/CE del Parlamento Europeo y del Consejo de 13 de diciembre de 1999, cuya regulación parte de una posición de neutralidad tecnológica que explica la excesiva generalidad antes resaltada. Esta toma de postura supone, como ha destacado Martínez Nadal, que no se hayan regulado de forma completa aspectos sustanciales de la firma digital –probablemente la única segura a día de hoy– y, sobre todo, que no se excluyan aquellas «técnicas y procedimientos que, en realidad no tiene[n] valor ni eficacia alguna»[96].

En definitiva, el amplio concepto legal de firma electrónica permite abarcar otras modalidades basadas en técnicas distintas de la criptografía asimétrica, ya disponibles, en desarrollo o futuras, que permitan cumplir algunas o todas las funciones características de las firmas manuscritas en un medio electrónico[97]. En concreto, según el artículo 3.1 de la LFE, se considera firma electrónica «el conjunto de datos en forma electrónica, consignados junto a otros o asociados con ellos, que pueden ser utilizados como medio de identificación del firmante». Así pues, en él tendrían cabida técnicas

---

22 de junio, de Acceso Electrónico de los Ciudadanos a los Servicios Públicos, 3ª ed., Thomson-Aranzadi, Madrid, 2010, p. 509].

[96] A. Martínez Nadal, *Comentarios*…, ob. cit., p. 81.

[97] Señala Linares que la equiparación que con cierta frecuencia se da en la práctica entre firma electrónica y firma electrónica avanzada o, en su caso, reconocida, trae causa de la existencia de criterios de clasificación distintos, el técnico y el jurídico, lo que ha dado lugar a una sinécdoque bastante generalizada [M. Linares Gil, «Identificación y autenticación de las Administraciones Públicas», en E. Gamero Casado y J. Valero Torrijos (coords.), *La Ley de Administración electrónica. Comentario sistemático a la Ley 11/2007, de 22 de junio, de Acceso Electrónico de los Ciudadanos a los Servicios Públicos*, 3ª ed., Thomson-Aranzadi, Madrid, 2010, p. 424].

tan simples como un nombre de usuario, una contraseña u otro elemento identificativo –por ejemplo la firma manual digitalizada– incluido al final de un mensaje o documento electrónico. Ahora bien, desde una estricta consideración técnica, tales instrumentos presentan un grado de fiabilidad diverso que habrá de precisarse en función de las garantías específicas que ofrezcan; de ahí que las disposiciones legales establezcan otros dos tipos de firma electrónica basados, en este caso, en el uso de técnicas criptográficas, modalidad que se conoce con la denominación de *firma digital*. Sin embargo, este último concepto no ha sido reconocido expresamente por el legislador que, por su parte, se refiere a las firmas electrónicas avanzada y reconocida.

De este modo, la firma electrónica avanzada sería aquélla que, según el artículo 3.2 LFE, «permite identificar al firmante y detectar cualquier cambio ulterior de los datos firmados, que está vinculada al firmante de manera única y a los datos a que se refiere y que ha sido creada por medios que el firmante puede mantener bajo su exclusivo control». Se trata, por tanto, de una categoría especial de firma electrónica que, no obstante, ha de cumplir una serie de requisitos concretos en base a los cuales se le reconoce una singular eficacia en la medida que ofrece mayores niveles de seguridad en la identificación del signatario y en la integridad de los documentos firmados con ella. En efecto, con las tres primeras exigencias –identificación del signatario, creación por medios bajo su exclusivo control y vinculación única al mismo– se persigue garantizar la autenticación y evitar el rechazo en origen de los mensajes electrónicos; mientras que con el último requisito –vinculación a los datos que permite detectar cualquier alteración ulterior–

se pretende salvaguardar la integridad de los documentos electrónicos.

Por tanto, esta pluralidad de firmas electrónicas requiere una aclaración previa que evite confusiones terminológicas que, en última instancia, generen dudas en cuanto a la eficacia jurídica de cada uno de los instrumentos analizados. En efecto, como señalábamos anteriormente, una clase particular de firma electrónica que cumpliría con los requisitos de autoría e integridad establecidos para la avanzada es la denominada *firma digital*, esto es, aquélla basada en una tecnología específica en la medida que se genera a partir de un sistema de criptografía asimétrica o de clave pública, lo que nos permite diferenciarla de la firma electrónica simple. En concreto, este sistema parte de la existencia de una clave de firma o clave privada, que únicamente conoce su titular y que permanece bajo su exclusivo control; y una clave pública a la que, por el contrario, puede acceder cualquier persona, si bien a través de la combinación matemática de ambas claves puede asegurarse de modo fidedigno que quien firma digitalmente un documento es realmente quien dice ser y que el contenido del mismo no ha sido alterado ni conocido por una tercera persona, sin que pueda obtenerse la clave privada a partir de la clave pública. Más aún, cuando la avanzada reúne determinadas garantías técnicas adquiere la condición de firma electrónica reconocida, debiendo a tal efecto –artículo 3.3. LFE– estar «basada en un certificado reconocido y generada mediante un dispositivo seguro de creación de firma».

¿Qué consecuencias jurídicas plantea esta distinción desde la perspectiva de la eficacia predicable respecto de cada una de estas modalidades?

b) La distinta eficacia de los tipos de firma electrónica y su proyección sobre los documentos electrónicos de las Administraciones Públicas

El análisis de la eficacia jurídica de la firma electrónica debe partir de una elemental premisa normativa: aun siendo la más extendida y, por tanto, un estándar de facto, la regulación legal no alude expresamente a la *firma digital* sino que parte de un concepto más amplio –la firma electrónica–, planteamiento que como antes señalábamos se justifica en base a la neutralidad tecnológica que debe predicarse respecto de este tipo de normas, ya que su efectividad se encuentra condicionada en última instancia por su mayor o menor grado de adaptabilidad a los incesantes avances que se van produciendo en este campo. Por tanto, el concepto legal de firma electrónica permite abarcar otras modalidades basadas en técnicas distintas de la criptografía asimétrica, ya disponibles o en desarrollo que permitan cumplir algunas o todas las funciones características de las firmas manuscritas en un medio electrónico. Ahora bien, dado que las garantías que ofrecen los diversos tipos de firma amparados por la definición legal no pueden equipararse, su eficacia jurídica también es necesariamente diversa.

Así, por lo que se refiere a la que podríamos denominar firma electrónica *simple*, es decir, la que no sea *avanzada* ni *reconocida*, podría ser considerada en principio y con carácter general como un instrumento inadecuado por cuanto, a tenor de lo dispuesto en el artículo 3 LFE, sólo garantiza la identidad del autor pero en modo alguno la integridad de la información. Ahora bien, teniendo en cuenta la prohibición *ex* artículo 3.9 LFE, no podrán negarse «efectos jurídicos a una firma electrónica que no reúna los requisitos de firma

electrónica reconocida en relación a los datos a los que esté asociada por el mero hecho de presentarse en forma electrónica», de manera que es necesario plantearse cuál sería la eficacia de un documento administrativo cuando se utilice esta modalidad de firma electrónica.

Se trataría, en definitiva, de dar una respuesta a ciertas prácticas muy frecuentes en el día a día de la actividad administrativa como, por ejemplo, la incorporación a los documentos administrativos de firmas manuscritas digitalizadas o la utilización de sistemas de seguridad basados en un nombre de usuario y una contraseña, que en principio no asegurarían de forma razonable por sí mismos la integridad de la información y, en el primer caso, ni siquiera la autoría por parte del titular de la firma, por cuanto cualquiera podría suplantarle sin mayores dificultades. Aunque esta problemática nos remite, en definitiva, a cuestiones fácticas que han de ser analizadas desde la perspectiva de la valoración de la prueba, no es menos cierto que el artículo 45.5 LRJAP requiere inexcusablemente como requisito de validez que se asegure la autenticidad e integridad del documento administrativo electrónico, exigencias que no se darían necesariamente cuando se hubiese empleado la modalidad de firma electrónica que nos ocupa. O, para ser más precisos, nos podríamos encontrar ante una potencial divergencia entre el contenido del documento y la voluntad real del órgano administrativo, autoridad o funcionario público que aparentemente lo suscribe, de ahí que, en principio, deba rechazarse la utilización de los referidos ejemplos de firma electrónica *simple* para los documentos administrativos ya que, en última instancia, se podría estar facilitando la revisión encubierta de decisiones sin respetar

los procedimientos legales de revisión que, en el caso de los actos administrativos, se establecen en los artículos 102 y ss. LRJAP. En consecuencia, los efectos jurídicos de los documentos que utilicen esta modalidad de firma electrónica dependerán, en última instancia y en caso de una eventual impugnación, de las garantías técnicas que ofrezca a la hora de asegurar la integridad y autenticidad del documento signado con ella, así como la autoría del mismo. En todo caso, desde la perspectiva de la innovación tecnológica, la utilización de sistemas de firma electrónica no basados en la criptografía asimétrica resulta manifiestamente insuficiente, en particular debido a los graves problemas de seguridad jurídica que se podrían plantear de forma reiterada en cuanto a la integridad y autenticidad de las actuaciones administrativas en general y de la información y los datos sobre los que se basen en particular.

De este modo, la plena validez y eficacia del documento administrativo electrónico nos remite necesariamente a la utilización de firma electrónica avanzada o reconocida, siendo también admisible el empleo de los mecanismos de identificación y autenticación enumerados en el artículo 13.3 LAE y regulados en el artículo 20 LAE. Ambos preceptos admiten expresamente que en el caso de relaciones entre Administraciones Públicas o, incluso, entre órganos pertenecientes a la misma entidad, se puedan realizar intercambios electrónicos de datos en entornos cerrados de comunicación, a los efectos de identificación de los sujetos que intervienen en la transmisión o, en su caso, el acceso y autenticación de los documentos electrónicos que produzcan. Ahora bien, aun cuando de una primera lectura de los referidos preceptos pudiera concluirse inicialmente que la validez y eficacia

de los documentos que se transmitan –de los datos o la información, en puridad– dependerá de lo acordado entre las partes que participan en la comunicación, lo cierto es que el pacto habrá de partir de la elemental premisa del respeto de las condiciones técnicas antes analizadas y, por tanto, aquéllas únicamente podrían fijar las circunstancias concretas, técnicas y organizativas, en que habrá de tener lugar la comunicación.

A este respecto, sólo la firma reconocida tiene asegurada de forma expresa –artículo 3.4 LFE– para los datos consignados en forma electrónica la equiparación a la firma manuscrita respecto de los datos consignados en soporte papel, lo que nos lleva a plantearnos cuál sería la eficacia de las otras dos modalidades de firma electrónica contempladas legalmente, es decir, la avanzada y la simple. Por lo que se refiere a la primera, debemos recordar que, según la definición legal, no sólo permite identificar al firmante y detectar cualquier cambio ulterior del documento sino que, incluso, ha de estar vinculada al firmante de manera única y a los datos a que se refiera, de manera que al haber sido generada por medios que aquél mantiene bajo su exclusivo control podría concluirse que, en última instancia, su eficacia también se puede equiparar a la propia de la firma manuscrita.

A la vista de tales afirmaciones, ¿dónde está pues la diferencia en el alcance de la regulación legal por lo que se refiere a las modalidades analizadas y, en concreto, a la firma avanzada? Se trata, en definitiva, de un problema relacionado con la prueba que ha de practicarse en el supuesto de que se niegue la autenticidad de la firma electrónica con la que se hayan signado los datos incorporados a un documen-

to electrónico[98], de manera que según el artículo 3.8 LFE debería distinguirse en función del tipo de que se trate. Así, en el supuesto de que fuese reconocida, quien haya presentado el documento deberá demostrar que la firma cumple con los requisitos establecidos para la avanzada y, además, que está basada en un certificado reconocido que reúne todos los requisitos previstos legalmente y, por último, que se ha generado mediante un dispositivo seguro de creación de firma; de manera que los gastos y costas que se generen corresponderán a quien hubiese formulado la impugnación en el caso de ser rechazada.

Por el contrario, si la firma sólo fuese avanzada resultarán de aplicación las reglas generales previstas por el artículo 326.2 de la Ley de Enjuiciamiento Civil para la fuerza probatoria de los documentos privados[99], de manera que quien hubiere presentado el documento podrá proponer las pruebas que estime pertinentes. En este caso, se plantea una doble alternativa:

---

[98] En palabras de I. Alamillo Domingo, la diferencia radica en el «grado de definición de los aspectos a comprobar en la pericial informática, que en el caso de la firma electrónica reconocida facilita la preparación de la prueba y, en su caso, la anticipación de la misma, y que además establece la presunción de autenticidad de la firma electrónica reconocida una vez verificada» [«Seguridad y firma electrónica: marco jurídico general», en E. Gamero y J. Valero (coords.): *Las Tecnologías de la Información y la Comunicación en la Administración de Justicia*, Thomson-Aranzadi, Cizur Menor, 2012, p. 428].

[99] Cfr. I. Alamillo Domingo, «Seguridad y firma electrónica…», ob. cit., p. 427. Como advierte A. Martínez Nadal, las modalidades de firma electrónica no reconocida implicarán que, en caso de impugnación, «sea necesario demostrar, a través de procedimientos probatorios en ocasiones difíciles y costosos, sus efectos respecto de la autoría e integridad del mensaje firmado» (*Comentarios*…, ob. cit., p. 93).

- que el órgano judicial concluya que el documento es auténtico, supuesto en el que procede igualmente la imposición de los gastos y costas para quien hubiere formulado la impugnación;

- que, por el contrario, entienda que no puede afirmarse su autenticidad, de manera que realizará la valoración de la prueba conforme a las reglas de la sana crítica, criterioo que también se habrá de aplicar en aquellos supuestos en que no se hubiere propuesto prueba alguna.

Ahora bien, este planteamiento general se encuentra condicionado en relación con los documentos generados por las Administraciones Públicas, ya que según el artículo 57 LRJAP los actos administrativos se presumen válidos y, en consecuencia, su eventual impugnación requiere desarrollar la correspondiente actividad probatoria tendente a desmontar la validez del sistema de firma electrónica empleado. En última instancia, la carga de la prueba –al menos inicialmente– se trasladaría a quien negase los efectos jurídicos al sistema de firma electrónica utilizado en ese concreto supuesto.

c) Las singularidades de la regulación de la firma electrónica en el ámbito de las Administraciones Públicas

Una de las principales novedades que ha introducido la LAE[100] en materia de identificación y autenticación de la actuación administrativa en general y, en particular, por lo que se refiere a los documentos administrativos, es la posibilidad de emplear diversos mecanismos en función de que el documento se genere de forma automatizada o directamente por una persona física, ya sea el titular de un órgano administrativo o simplemente el personal al servicio de la Administración Pública autora del documento. Procede, pues, que analicemos las diversas hipótesis que pueden plantearse por lo que se refiere a la utilización de cada uno de estos sistemas en relación con los documentos administrativos.

En efecto, junto a las citadas disposiciones de carácter general ya analizadas, en el ámbito de las Administraciones Públicas se han dictado normas específicas para regular la utilización de la firma electrónica en la actividad de las mismas y sus relaciones con los ciudadanos. En concreto, los artículos 13 a 23 LAE han incorporado previsiones particulares al respecto, junto con algunas otras que indirectamente se refieren a la exigencia de su utilización, tal y como sucede singularmente con las disposiciones reguladoras de la sede electrónica –artículo 10– o el documento administrativo

[100] Para una visión general sobre las singularidades de la firma electrónica en la regulación de la normativa sobre Administración electrónica, al margen de las obras citadas en las notas anteriores, véase R. Martínez Gutiérrez, «Identificación y autenticación: DNI electrónico y firma electrónica», en J. L. Piñar Mañas (dir.), *Administración electrónica y ciudadanos*, Civitas-Thomson Reuters, Cizur Menor, 2011, pp. 407-453.

–artículos 29 y 30–. Si bien la mayor parte de tales preceptos tienen carácter básico y, en consecuencia, resultan de aplicación a todas las Administraciones Públicas, debe tenerse en cuenta que también se han dictado normas que desarrollan las previsiones de la LAE en cada Administración Pública, de manera que pueden incorporar disposiciones específicas al respecto, tal y como sucede con el RLAE en la Administración General del Estado, cuyo Título III se dedica específicamente a la identificación y autenticación. Ahora bien, esta última circunstancia ha de ser valorada con cierta prevención y con un alcance restrictivo, de manera que no se desnaturalice la regulación general básica. En efecto, en base al ejercicio de las competencias autonómicas de desarrollo y, asimismo, a las relativas a la autoorganización de comunidades autónomas y entidades locales se podrían establecer diferencias en el régimen jurídico aplicable que, en definitiva, supusieran una dificultad a la hora de aplicar criterios estandarizados de interoperabilidad que faciliten la gestión documental avanzada y el ejercicio de los derechos de los ciudadanos a no tener que reiterar la presentación de documentos en poder de las Administraciones Públicas.

Quizás la principal característica a destacar de la regulación legal en materia de Administración electrónica sea la continua referencia que en la LAE se hace a la firma electrónica avanzada y no a la reconocida[101] que, en función de

[101] I. Alamillo Domingo y X. Uríos Aparisi, «El nuevo régimen legal de gestión de la identidad y firma electrónica por las Administraciones Públicas», en L. Cotino y J. Valero (coords.), *Administración electrónica. La Ley 11/2007, de 22 de junio, de Acceso Electrónico de los Ciudadanos a los Servicios Públicos y los retos jurídicos del e-gobierno en España*, Tirant lo Blanch, Valencia, 2010, p. 665, quienes llegan incluso a considerar que se ha producido una «degradación de

lo previsto en el artículo 3.4 LFE, es la única que tiene garantizada legalmente de forma expresa la equivalencia con la firma manuscrita desde el punto de vista de su eficacia; sin perjuicio de que a la primera no se le pueda privar de efectos jurídicos al amparo del artículo 3.9 LFE, tal y como ya se explicó con anterioridad.

Desde esta amplia perspectiva, el artículo 13.3 LAE expresamente habilita a que las Administraciones Públicas utilicen tanto certificados de dispositivo seguro para identificar su sede electrónica, sistemas de firma electrónica para las actuaciones automatizadas, la firma electrónica de su personal y, en su caso, el DNI electrónico, así como el intercambio electrónico de datos cuando se acuda a sistemas cerrados de comunicación. Igualmente, se reconoce de forma expresa la posibilidad de que en las actuaciones automatizadas –artículo 18 LAE– se empleen tanto sellos electrónicos basados en sistemas de firma electrónica como códigos seguros de verificación, correspondiendo a cada Administración la determinación de los casos en que procederá un instrumento u otro. Mientras que en el primer supuesto se establece una obligación de publicidad electrónica de la relación de sellos utilizados y la de poner a disposición los medios que permitan la verificación de los mismos, en el segundo será imprescindible ofrecer un sistema telemático de consulta a través de la sede electrónica mediante el cual se permita comprobar la integridad del documento, por lo que puede afirmarse que en la *mens legis* este último medio está concebido como una herramienta vinculada a la comprobación de la autenticidad

---

la firma electrónica reconocida como nivel normal de seguridad en las relaciones con las Administraciones Públicas».

de las copias de los documentos administrativos, especialmente cuando se encuentren en soporte papel.

Más allá de la diferente virtualidad y eficacia de ambos instrumentos, una aparente cuestión de matiz ha de ser destacada por cuanto podría pasar desapercibida a pesar de su relevancia práctica: en ambos casos se hace una referencia expresa a que el sello y el código pueden estar vinculados no sólo a un órgano concreto sino, más genéricamente, a la entidad en su conjunto; de manera que se está produciendo un desplazamiento de la titularidad competencial desde los órganos hasta las personas jurídicas en que se integran, con lo que se pretende facilitar la realización automatizada de ciertas actuaciones sin necesidad de una intervención humana directa. Ahora bien, en todo caso esta pretensión no puede ser contraria a las normas reguladoras de la Administración correspondiente en cuanto realicen atribuciones competenciales a favor de órganos concretos –por ejemplo, si atribuyen a un determinado órgano la relativa a la expedición de copias auténticas– y, asimismo, ha de respetar las exigencias –en este caso, también competenciales– a que se refiere el artículo 39 LAE y que no corresponde ahora analizar en profundidad. Esta última premisa ha de asegurarse igualmente cuando se utilicen sellos electrónicos vinculados únicamente al órgano competente y no a la persona física de su titular; es decir, que no supongan que este último deba hacer uso personal y directo del correspondiente certificado, a pesar de lo cual la actuación se entenderá realizada por el órgano, si bien de manera automatizada.

Supuesto distinto es, por el contrario, aquél en que las personas físicas –ya sean titulares de órganos, ya de unidades administrativas o, simplemente, personal al servicio de la

Administración– empleen sus propios certificados electrónicos, instrumentos a los que preceptivamente habrá de acudirse cuando sea necesaria la identificación y autenticación del ejercicio de la competencia y no se trate de actuaciones automatizadas, es decir, cuando la decisión deba ser adoptada de forma directa por una persona física. En este caso, las Administraciones Públicas pueden decidir tanto que se empleen sistemas específicos que identifiquen no sólo a la persona física sino, asimismo, el cargo o puesto que ocupa en la organización administrativa como, en su caso, facilitar el uso de la firma vinculada al DNI electrónico, posibilidad admitida expresamente por el artículo 19.3 LAE. Sin embargo, esta habilitación legal no empece para que deban respetarse los principios generales vigentes en materia de protección de datos personales y, en concreto, el relativo a la calidad –artículo 4 LOPD– en su manifestación de que el tratamiento de los mismos sea proporcionado. En efecto, «una cosa es que se utilice el DNI electrónico para la identificación de su titular y otra muy distinta que en cualquier supuesto el documento firmado deba hacer referencia expresa al número de identificación fiscal –NIF– asociado, revelación que no tiene lugar cuando las autoridades y el personal al servicio de las Administraciones Públicas firman manuscritamente un documento en soporte papel: ¿qué justificación puede amparar esta dualidad?»[102]. Y, por tanto y como consecuencia inescindible, tampoco esta información podría incorporarse a los metadatos asociados a los documentos electrónicos aun cuando dicha información personal no aparezca recogida en el cuerpo principal de aquéllos ya que, en definitiva, el

[102] J. Valero Torrijos, «El alcance de la protección…», ob. cit., p. 158.

sistema de gestión innovadora en que se basa su utilización permite acceder, conocer e, incluso, llevar a cabo tratamientos avanzados de tales datos aunque, en apariencia, dicha información no sea revelada como parte del contenido del documento. De este modo, la adecuada protección del citado derecho fundamental requeriría que los programas y aplicaciones que se utilicen para generar el correspondiente documento administrativo electrónico sean diseñados conforme a esta exigencia; sin perjuicio, claro está, de que deban llevarse a cabo las comprobaciones oportunas en orden a la validación del estado de los certificados, lo que no implica necesariamente revelar a terceros cierta información personal, como es el caso del número de identificación antes aludido.

Asimismo, cabe la posibilidad de que la Administración Pública en que se integra el autor del documento electrónico haya aprobado normas o criterios que redunden en el establecimiento de requisitos adicionales para el uso de la firma electrónica y, en concreto, para el empleo de certificados *profesionales* que acrediten no sólo la identidad sino también la condición subjetiva de personal o autoridad al servicio de la misma[103]. En estos casos, además de las anteriores exigencias de carácter general relativas a la comprobación del estado de revocación del certificado, por lo que respecta a la identidad del titular también deberían añadirse las específicamente referidas a su condición subjetiva, de manera que podría darse

---

[103] En relación con la acreditación de dicho elemento subjetivo, más allá de los llamados *certificados de atributos*, véanse las sugerentes reflexiones de I. Alamillo Domingo y X. Uríos Aparisi, «La gestión de identidades y capacidades por las Administraciones Públicas», *IX Jornadas Tecnimap*, Sevilla, 2006, pp. 5 y 6.

el caso de que el certificado no hubiese sido revocado pero su titular no ocupe ya el cargo que conste en el mismo. Este eventual desfase justificaría la preferencia por los sistemas de comprobación dinámica de los atributos al margen de los propios certificados electrónicos, lo que sin duda conlleva una mayor complejidad en cuanto a la gestión de su validación pero, no obstante, permite incrementar la seguridad jurídica y ofrecer servicios de valor añadido respecto de la gestión documental basada en el soporte papel. En efecto, se trata de un claro ejemplo que evidencia cómo la tecnología puede ofrecer mayor seguridad en términos jurídicos a partir de un modelo avanzado de gestión de identidades por cuanto, en definitiva, cuando el titular de un órgano administrativo o un funcionario público firman un documento en soporte papel no tiene lugar comprobación alguna sobre la vigencia o no de su condición subjetiva o, al menos, tal actividad no se realiza más que a *posteriori*, una vez detectado un posible problema. Por el contrario, el sistema asociado a certificados electrónicos supone que automáticamente se pueda llevar a cabo dicha constatación, lo que obliga en definitiva a adoptar las medidas técnicas y organizativas que permitan aprovechar tal potencialidad innovadora.

En todo caso, la elección de una u otra modalidad de identificación del personal corresponde en gran medida a cada Administración Pública, ya a través de una regulación específica de desarrollo ya en función de criterios fijados al margen de disposiciones normativas, de manera que siempre que se cumplieran las exigencias básicas que establecen la LAE o la legislación estatal sobre firma electrónica la entidad destinataria del documento no podría discutir su validez y eficacia, tal y como dispone el artículo 4.e) LAE.

d) Las comprobaciones relativas al uso de la firma electrónica en la gestión documental: problemas y disfunciones derivados de la intermediación de prestadores de servicios de certificación

Según se desprende del artículo 3.2 y 3 LFE, tanto la firma electrónica avanzada como la reconocida permitirían acreditar no sólo la identidad del firmante sino, adicionalmente y a diferencia de la simple, también detectar «cualquier cambio ulterior de los datos firmados», dando satisfacción por tanto a las exigencias de integridad y autenticidad planteadas por el artículo 45.5 LRJAP. Sin embargo, el funcionamiento pleno y satisfactorio de este tipo de sistemas suscita una serie de problemas específicos a los que debe darse solución no sólo desde la tecnología sino, antes bien y por lo que afecta al presente trabajo, desde la perspectiva jurídica. De lo contrario no se podría aprovechar plenamente el potencial de aquélla como instrumento para reforzar la seguridad jurídica de la innovación basada en sistemas dinámicos y avanzados de comunicación con los ciudadanos y de gestión documental.

En primer lugar, existe una obligación de aceptar aquellos documentos administrativos emitidos por otras Administraciones Públicas que hubieran sido firmados digitalmente utilizando los servicios de certificación ofrecidos por cualquier proveedor que satisfaga las exigencias técnicas que, a tal efecto, se establecen en la legislación de firma electrónica: se trata de una consecuencia ineludible a la vista del principio de libre prestación de servicios de certificación que, por imposición de la normativa europea en la materia, reconoce el artículo 5 LFE, incluso si los citados prestadores se encontraran establecidos en otro Estado de la Unión

Europea. Al margen de los problemas técnicos y organizativos que la aplicación efectiva de este principio conlleva[104], la admisibilidad de tal número y diversidad de certificados supone un inconveniente práctico relevante, sobre todo por la exigencia de comprobar su vigencia –y, en su caso, la relativa a los atributos del titular del órgano, autoridad o funcionario signatario– en el momento de la fecha que aparece reflejada en el documento administrativo.

Este inconveniente se encuentra reduplicado por lo que se refiere a los servicios ofrecidos por la FNMT, prestador mayoritario en el ámbito del sector público que normalmente opera a través de convenios con las respectivas Administraciones Públicas, en virtud de los cuales los servicios de validación sólo se encuentran accesibles previa satisfacción de una cierta cantidad económica. Se trata de un modelo de negocio basado en el pago por el destinatario de los documentos firmados y no por parte de quien los firma[105], que es en realidad a quien se le presta el servicio, cuya conformidad con el artículo 21 LAE es más que dudosa; y, en última instancia, impide aprovechar el valor añadido que, desde el punto de vista de la seguridad jurídica, ofrece la herramienta tecnológica referida para asegurar tanto la identidad de los sujetos que intervienen como la integridad y la autenticidad de los documentos y datos utilizados, entorpeciendo las co-

---

[104] Cfr. I. Martín Delgado, «Identificación y autenticación…», ob. cit., pp. 516 a 522.

[105] Ciertamente, el impulso que ha recibido el uso de los certificados en el ámbito de la Administración electrónica gracias al impulso de la FNMT no puede ser obviado, pero lo cierto es que desde la perspectiva de la regulación vigente el modelo de negocio en que se basa su actividad es más que discutible. En relación con esta idea, cfr. R. Couto Calviño, *Servicios de certificación de firma electrónica y libre competencia*, Comares, Granada, 2008, pp. 88 a 91.

nexiones automatizadas de información con plenas garantías desde la perspectiva del Derecho. En efecto, según el citado precepto, los certificados reconocidos sólo serán admitidos cuando el prestador ponga a disposición de la Administración Pública la información precisa en condiciones técnicamente viables y sin coste alguno para ella, de manera que la conclusión parece evidente: la negativa de la FNMT a ofrecer servicios de validación de forma gratuita a terceras entidades en relación con los documentos firmados por aquellas Administraciones Públicas que sí tienen suscrito un convenio con ella es contraria a lo dispuesto en el citado precepto legal.

En todo caso, este problema debería solventarse de forma definitiva obligando a todos los prestadores y, en concreto a la FNMT, a que permitan el libre acceso a la información necesaria para comprobar el estado del certificado en el momento de ser utilizado respetando las condiciones a que se refiere el artículo 21 LAE, es decir, sin coste alguno para la Administración Pública destinataria del documento[106]. Precisamente, el artículo 21.3 LAE pretende establecer el mecanismo oportuno a tal efecto al disponer que la Administración General del Estado ofrezca una plataforma de «ve-

[106] Cfr. A. Martínez Nadal, *Comentarios*..., ob. cit., p. 341, quien admite que, desde la perspectiva del régimen general de la LFE, el prestador pueda cobrar una tasa para acceder a la lista de certificados revocados. No obstante, dada la exigencia establecida en el ámbito de la Administración electrónica, la posibilidad de condicionar el acceso al servicio de validación al pago de cantidad alguna ha de entenderse circunscrita a que la Administración Pública que utilice los certificados satisfaga las cantidades que procedan en su relación contractual –o convencional– con el prestador, pero en modo alguno a los ciudadanos u otras entidades públicas que deban comprobar la vigencia del certificado utilizado para, de esta manera, confiar en la validez y eficacia del documento electrónico.

rificación del estado de revocación de todos los certificados admitidos en el ámbito de las Administraciones Públicas que será de libre acceso por parte de todos los Departamentos y Administraciones». Aun cuando ya se encuentra operativo este servicio respecto de todos los certificados admitidos en el ámbito de las Administraciones Públicas a través de varias vías, en uno de los casos la comprobación ha de hacerse individualmente para cada uno de los certificados[107] y, por lo que respecta al servicio que se permite para las Administraciones Públicas[108], la comprobación automatizada y masiva del estado de los certificados se ofrece, en principio, a través de un servicio disponible en condiciones jurídicas tales que conllevan el pago de la contraprestación prevista en el respectivo contrato o convenio[109]. Difícilmente cabe, por tanto, admitir la consecuencia de que, debido la imposibilidad jurídica de llevar a cabo las comunicaciones que han de tener lugar para realizar las comprobaciones exigidas por la singularidad en el funcionamiento de la firma digital, las mismas no se ejecuten y, por tanto, la gestión documental no se fundamente en la fortaleza que permite la tecnología, degradándose de este modo la seguridad jurídica reforzada que, en principio,

---

[107] https://valide.redsara.es/ (última visita: 15/09/2012).

[108] http://www.cert.fnmt.es/convenio/dpc.pdf (última visita: 15/09/2012).

[109] Se trata de la herramienta @firma, accesible en http://administracionelectronica.gob.es/ desde las secciones Firma Electrónica y CTT (última visita: 15/09/2012). Sin embargo, por lo que se refiere a la utilización de @firma en relación con los certificados expedidos por la FNMT, las condiciones se han de fijar a través del correspondiente contrato o convenio, es decir, mediante la oportuna contraprestación. En relación con esta última exigencia, véanse los apartados 9.13 y 9.14 de la *Declaración de Prácticas de Certificación* de la FNMT, versión 2.8, accesible desde http://www.cert.fnmt.es/convenio/dpc.pdf (última visita: 15/09/2012).

y de no admitirse dichas restricciones, podría obtenerse. En otras palabras, es jurídicamente inadmisible cualquier pretensión de innovación que se fundamente en la reducción del nivel de garantía que ofrece la tecnología.

Al margen de las dificultades prácticas que estas condiciones suponen para el intercambio de documentos administrativos firmados electrónicamente dado el amplio número de Administraciones Públicas que utilizan los servicios de la FNMT, según se ha mantenido anteriormente, dicha práctica contraviene lo dispuesto en el artículo 21 LAE y, en definitiva, nos lleva a la inexorable conclusión de que los certificados de dicho prestador cuyo estado de revocación no se pueda comprobar gratuitamente no deberían ser admitidos por las Administraciones Públicas dado que no se puede confiar razonablemente –en puridad, no se puede comprobar– en su vigencia en el momento de ser utilizados.

En todo caso, más allá del supuesto concreto referido al citado prestador y desde una perspectiva internacional intensificada en los últimos años, el acceso a los servicios de validación a través de la plataforma ofrecida por la Administración General del Estado está llamado a jugar un papel decisivo con aquellos ciudadanos extranjeros que precisen relacionarse telemáticamente con una Administración española y, en ejercicio de sus derechos y en aplicación del principio de libre prestación de servicios fijado por la Directiva, decidan utilizar los certificados que les hayan sido expedidos en su país de origen. Se trata de un supuesto ciertamente frecuente en relación con aquellos ciudadanos de la Unión Europea que pasan sólo una parte del año en España, ya que en estos casos los inconvenientes derivados de las exigencias de interoperabilidad por lo que se refiere a la identificación

y autenticación sólo podrán ser en gran medida soslayados a través de esta herramienta de cooperación interadministrativa con el apoyo de iniciativas supranacionales similares a las que, bajo las siglas STORK[110], se pongan en marcha.

Nos encontramos, por tanto, ante dificultades específicas del funcionamiento de la firma electrónica como instrumento técnico que permite dotar de seguridad a la gestión documental avanzada que se lleve a cabo por medios electrónicos y, en concreto, de la necesaria participación de terceros intermediarios que, como en el supuesto que se acaba de exponer, pueden impedir que se realicen las comprobaciones exigidas para acreditar las condiciones jurídicas inexcusables a partir de las cuales construir la Administración electrónica. En última instancia, se trata de una consecuencia derivada de la transición de un modelo de identificación basado en el monopolio del sector público –y en concreto, de las autoridades policiales de cada uno de los Estados, al menos en la mayor parte de la Unión Europea– característico de las relaciones presenciales a otro en el que, como consecuencia de la liberalización impulsada desde el ámbito europeo, la intermediación se puede llevar a cabo incluso por entidades privadas, nacionales o pertenecientes a otro Estado, en un régimen de plena liberalización; lo que, en definitiva, obliga a una reconfiguración de los parámetros en base a los cuales se han construido tradicionalmente las relaciones entre los ciudadanos y las Administraciones Públicas. De lo contrario, la innovación tecnológica no será factible jurídicamente o, en su caso, sólo podrá plantearse degradando el respeto y la efectividad de las normas jurídicas.

---

[110] http://www.eid-stork2.eu/ (última visita: 15/09/2012).

e) Implicaciones jurídicas de los desajustes en la regulación de la firma electrónica como consecuencia de su singularidad tecnológica

Como acaba de explicarse, la firma digital implica la participación de una tercera parte de confianza, el prestador de servicios de certificación, cuya actividad incide indirectamente sobre la relación jurídica que se establece entre la Administración Pública y los ciudadanos cuando se utilizan medios electrónicos. Sin embargo, lejos de presentar una perspectiva estática como inicialmente pudiera parecer, la intervención de estas entidades conlleva una serie de singularidades que pueden afectar directamente a las condiciones jurídicas en que tienen lugar las actuaciones administrativas y las comunicaciones con los ciudadanos. Así, por aplicación del principio de libre prestación de los servicios de certificación consagrado en la normativa europea, cada ciudadano –y también las entidades públicas– puede elegir libremente la utilización de certificados expedidos por cualquier proveedor que cumpla con las exigencias técnicas fijadas legalmente, lo que conlleva la consiguiente obligación de aceptar las firmas electrónicas generadas a través de los mismos.

Ahora bien, la anterior conclusión parte de una premisa inexcusable: que pueda comprobarse el estado del certificado en el momento de ser utilizado y, en concreto, que el mismo no se encuentre revocado ya que, de ser así, no se debería confiar en la firma electrónica que se hubiese generado. Ahora bien, los propios prestadores han de permitir la validación por terceros en condiciones de interoperabilidad, de manera que si no lo hiciesen sería inviable realizar la comprobación anterior y, por tanto, no sería posible afirmar en términos jurídicos que el documento firmado o la actuación realizada

respeta las exigencias de integridad y autenticidad legalmente requeridas[111]. Nos encontramos ante un requisito que no se da en el ámbito de la gestión documental en soporte papel y las relaciones presenciales que, por tanto, se justifica por la singularidad de la tecnología en que se fundamenta la firma electrónica; pero, al mismo tiempo, es una demostración de cómo la tecnología puede reforzar las garantías jurídicas de la actuación realizada, ya que también en el caso de una firma manuscrita cabría comprobar su autenticidad a través de una prueba pericial, si bien en este caso sólo podría llevarse a cabo la verificación a *posteriori*, es decir, una vez consumado el ilícito.

Más allá de la problemática relativa a las condiciones económicas y jurídicas en que ha de tener lugar esta operación de verificación, lo cierto es que nos obliga a plantearnos la incidencia que tendría el uso de certificados revocados por parte de las autoridades administrativas. En principio, al no poder subsumirse en alguna de las causas de nulidad que contempla el artículo 62 LRJAP, cabría pensar que se trata de un supuesto de anulabilidad que admitiría la convalidación siempre que el titular del certificado se ratificase en su actuación. Sin embargo, el hecho de que el certificado ya no estuviera vigente no impide que la declaración de voluntad, juicio, conocimiento o deseo en que consiste el acto admi-

[111] En palabras de J. F. Ortega Díaz, se trata de una de las premisas esenciales para que el tercero verificador –en nuestro caso, la Administración Pública que recibe el documento generado por otro sujeto o entidad– confíe en una firma electrónica, de manera que el acceso a la información relativa a la validez resulta crucial, salvo en los supuestos en que la expiración del certificado se haya producido por el transcurso del tiempo de su vigencia (*La Firma y el Contrato de Certificación Electrónicos*, Thomson-Aranzadi, Cizur Menor, 2008, p. 123).

nistrativo reúna los requisitos generales exigibles sino que, simplemente, afecta a las condiciones de comprobación de la presunción legal en que se basa el uso de los certificados a los efectos de la imputación de la autoría del documento. En consecuencia[112], la imposibilidad de llevar a cabo la comprobación de forma gratuita no afectaría en sí misma a su validez sino, más bien, a su eficacia. En última instancia, salvo el matiz que más adelante se referirá, lo que no podría conocerse es si fue firmado empleando un certificado –y, por tanto, la clave privada asociada al mismo– que estuviera en vigor en el momento de utilizarse, de manera que la Administración Pública que recibe el documento electrónico firmado por otra no dispone de medios lícitos para hacer la comprobación en las condiciones del artículo 21 LAE y, en consecuencia, difícilmente pude hablarse de una obligación al respecto. Más aún, únicamente podría conocer si el certificado estaba o no caducado, ya que dicha información temporal sí consta en la información que el mismo proporciona, pero no si dicho certificado había sido revocado al margen de la anterior circunstancia y, en consecuencia, se encontraba en vigor al ser utilizado para signar electrónicamente el documento administrativo en cuestión. Incluso, resulta frecuente que esta comprobación se lleve a cabo por una nueva entidad que, de este modo, se interpondría entre la Administración Pública y el ciudadano e, incluso, el prestador de servicios de certificación, de manera que se conectaría con este último para prestar un servicio a aquélla en relación con la actuación realizada por el segundo. Sólo a partir de esta ma-

[112] Por lo que se refiere a esta argumentación, véase J. Valero Torrijos, «El alcance de la protección…», ob. cit., p. 160.

yor complicación puede comprenderse el alcance real de las implicaciones jurídicas que conlleva el uso de la firma digital como herramienta a través de la cual asegurar la integridad y autenticidad en relación con los servicios de Administración electrónica.

Ahora bien, sentada esa regla general hay que realizar una importante matización por lo que respecta a la comprobación del estado de los certificados que podría tener consecuencias invalidantes. Se trataría del caso en que su titular hubiese comunicado al prestador alguna circunstancia que determinase la revocación del certificado, de manera que si el mismo fuese utilizado por otra persona distinta de su titular concurriría una causa de nulidad radical –artículo 62.1.d) LRJAP– en la medida que la usurpación de identidad fuese constitutiva de infracción penal[113]. En este supuesto, la imposibilidad de llevar a cabo la validación impediría constatar el estado de revocación del certificado y, por tanto, la responsabilidad debiera ser asumida por el prestador al menos desde la perspectiva de la reparación de los daños que se pudieran causar. En consecuencia, la necesidad de comprobar el estado de los certificados se convierte en una exigencia inexcusable por parte de la Administración destinataria de los documentos electrónicos, a menos que se pretenda rebajar el nivel de garantía que ofrece esta tecnología. Des-

[113] Cfr. A. Palomar Olmeda, *La actividad administrativa*…, ob. cit., p. 287, quien añade que será el titular de la competencia administrativa y, en concreto, del certificado utilizado quien tenga que «probar la diligencia en la custodia de las claves, su denuncia ante las autoridades si se ha percatado de su utilización ilegal y, en general, mostrar una actitud que permita entender deshecha al presunción de que la actuación ligada a la firma electrónica corresponde al titular».

de la perspectiva de la interoperabilidad en términos jurídicos, debemos reiterar que existe una obligación de aceptar aquellos documentos emitidos por otras Administraciones Públicas que hubieran sido firmados digitalmente utilizando los servicios de certificación ofrecidos por cualquier proveedor que satisfaga las exigencias técnicas que, a tal efecto, se establecen en la legislación de firma electrónica[114]. Ahora bien, en puridad y salvo en los supuestos referidos, la imposibilidad de llevar a cabo dicha comprobación no afectaría en sí misma a la validez del documento electrónico ya que, en última instancia, simplemente se impediría constatar si el documento fue firmado utilizando un certificado –y, por tanto, por la persona física asociada al mismo– que estuviera en vigor en el momento de utilizarse. El problema se situaría, más bien, en el plano de la eficacia, ya que la Administración Pública que recibe el documento electrónico firmado por otra podría no disponer de medios lícitos para hacer la comprobación en las condiciones del artículo 21 LAE y, en consecuencia, difícilmente cabría plantear la existencia de una obligación al respecto.

Al margen de las implicaciones concretas en relación con la gestión documental y, en particular, la validez y eficacia de las actuaciones que se lleven a cabo sin realizar la comprobación referida, lo cierto es que se trata de particularidades propias únicamente de la firma *digital*, de manera que es necesario realizar una valoración más amplia desde la perspectiva general de la regulación de la firma electrónica y, en particular, desde la laxitud del concepto legal empleado y la diversidad tipológica reconocida. Como se ha destacado an-

[114] I. Martín Delgado, «Identificación y autenticación…», ob. cit., p. 519.

teriormente, la regulación del uso de la firma electrónica en el ámbito de las Administraciones Públicas se caracteriza por su flexibilidad, circunstancia que debe ser valorada positivamente en principio, sin perjuicio de algunas matizaciones[115].

En efecto, si bien la normativa contempla la utilización de otras modalidades de identificación y autenticación, su admisibilidad debe ser planteada de manera restrictiva y sólo en la medida que así se justifique por razones técnicas que fundamenten la seguridad jurídica en que se han sustentar las exigencias de integridad y autenticidad que reclama el interés público que podría verse afectado. Por tanto, el uso de firmas escaneadas debe ser en principio descartado, a menos que tales exigencias se vean satisfechas, lo que no podría suceder cuando se trate de actuaciones automatizadas ya que, en estos casos, procede la utilización de un sello de órgano; de manera que se reduciría a los supuestos en que no se diera dicha modalidad de actuación y la decisión se adoptase directamente por la persona física titular del órgano que, debido al elevado número de documentos a signar, podría utilizar esta modalidad de firma electrónica siempre y cuando se adopten las medidas que eviten la manipulación de su decisión a la hora de plasmarla documentalmente. Por lo que respecta a la posibilidad de utilizar –a los efectos de identificación y autenticación– otros sistemas como el intercambio electrónico de datos en entornos cerrados de co-

[115] En concreto, será necesario determinar caso por caso la concreta exigencia técnica y jurídica que se pretende satisfacer para decidir qué modalidad procede utilizar, de manera que, como tal y como advierte M. Linares Gil, la pluralidad admitida por el legislador plantea un evidente riesgo de dispersión y heterogeneidad a pesar de la ventaja de flexibilización que conlleva («Identificación y autenticación…», ob. cit., p. 426).

municación, sólo resultaría admisible en el supuesto de que previamente se hubiesen fijado las condiciones técnicas y las medidas de seguridad a respetar. Y en relación con la aparente preferencia del legislador por la firma avanzada frente a la mayor garantía que ofrece la reconocida, ciertamente se trata en última instancia de una cuestión sustancialmente de facilidad probatoria que no admite dudas en cuanto a su legalidad, si bien llama la atención que se apueste en el ámbito de las Administraciones Públicas por una modalidad que ofrece menores garantías jurídicas cuando, precisamente, el Estado provee a todos los ciudadanos con un instrumento como el DNI electrónico, cuya eficacia jurídica se encuentra reforzada. Sin duda, se trata de una decisión basada en razones de oportunidad y, en concreto, en facilitar la utilización de otros certificados también expedidos por prestadores del sector público que en modo alguno puede cuestionarse desde el punto de vista de su legalidad. Al menos en teoría, ya que debe recordarse que, al margen de la rebaja en las garantías técnicas que esta posibilidad conlleva, en la práctica las condiciones de validación de los certificados son ciertamente discutibles en algún caso.

2. LA RELEVANCIA JURÍDICA DE LAS EXIGENCIAS DE SEGURIDAD E INTEROPERABILIDAD EN LA ADMINISTRACIÓN ELECTRÓNICA

Al margen de las exigencias relativas a la gestión documental que se analizan en el siguiente capítulo, el legislador español ha otorgado carta de naturaleza normativa a una serie de requisitos mínimos y principios básicos a los que se

ha de someter cualquier proyecto y servicio de Administración electrónica a fin de permitir la protección adecuada de la información y, por lo que respecta a la interoperabilidad, facilitar su gestión, conservación y normalización, así como de los formatos y de las aplicaciones: son los denominados esquemas nacionales de Seguridad, contemplado en el artículo 42 LAE y regulado mediante Real Decreto 3/2010, de 8 de enero, y de Interoperabilidad, cuyas previsiones han sido aprobadas mediante Real Decreto 4/2012, de idéntica fecha. En consecuencia, no se trata simplemente de meras recomendaciones y criterios programáticos cuya efectiva aplicación quede en manos de las respectivas Administraciones Públicas sino que, por el contrario, constituyen auténticas normas jurídicas cuya infracción no puede quedar simplemente en el ámbito del incumplimiento de buenas prácticas, hasta el punto de que podría afectar incluso a la validez de las actuaciones que se lleven a cabo utilizando medios electrónicos.

Esta afirmación se encuentra reforzada en la medida que ambos esquemas constituyen normas de carácter básico según la disposición final primera LAE, de manera que incluso el legislador autonómico o las normas que dicten las entidades locales han de respetar sus previsiones. En consecuencia, su carácter normativo está fuera de toda duda, por lo que la totalidad de las Administraciones Públicas habrán de ajustarse a sus previsiones en los términos que analizaremos a continuación. A este respecto es necesario advertir que, aun cuando hayan sido aprobados mediante norma reglamentaria estatal, en su elaboración han participado las comunidades autónomas y las entidades locales, siendo elaborado el proyecto inicial en el seno de la Conferencia Sectorial de Administración Pública y contado con el infor-

me favorable de la Comisión Nacional de Administración Local.

Se trata de un matiz relevante, ya que en ambos casos su ejecución conlleva la adopción de medidas organizativas que, en principio, corresponderían a la competencia de cada entidad, soslayándose de esta manera este inconveniente jurídico-formal; sin perjuicio de que, en la valoración concreta de su alcance, debe concluirse la dificultad que supone su cumplimiento para buena parte de los municipios, inconveniente que, sin embargo, no puede convertirse en excusa para dejar de exigir su efectivo cumplimiento. En consecuencia, el respeto a las previsiones de los citados esquemas constituye una premisa inexcusable a la hora de afrontar la adaptación de los procedimientos administrativos a las previsiones de la LAE por parte de todas las Administraciones Públicas, de manera que en el caso autonómico y local las «disponibilidades presupuestarias» –disposición final tercera LAE– deben contemplar necesariamente su cumplimiento, sin que puedan ponerse en marcha trámites y actuaciones que no respeten sus exigencias.

No obstante, incluso cuando se haya contado con el visto bueno de los órganos representativos antes referidos, lo cierto es que en relación con la dimensión y los medios de algunas entidades municipales su cumplimiento podría parecer desproporcionado y, en consecuencia, surgir la tentación de obviar su respeto o, al menos, proceder a una aplicación limitada de sus previsiones. Ahora bien, por las razones antes aludidas y, en general, debido a los problemas jurídicos tan serios que podrían generarse de incumplirse tales criterios tecnológicos, esas opciones han de ser descartadas radicalmente, de manera que procedería la actuación colaborativa

de las propias Administraciones o, en su caso, que las entidades territoriales superiores les proporcionen los medios para su efectivo respeto, tal y como prevé la propia disposición final tercera LAE para el ámbito local.

Veamos pues cuál es el alcance de tales esquemas desde el punto de vista de su contenido material más allá de la problemática formal referida a la perspectiva competencial examinada.

a) El Esquema Nacional de Seguridad

La seguridad es uno de los pilares basilares a partir del cual se articula la Administración electrónica, tal y como demuestra el hecho de que, al margen de declaraciones implícitas –caso, por ejemplo, del artículo 1.2 LAE al fijar los objetivos de la Ley–, se encuentre expresamente consagrada entre las finalidades –artículo 3 LAE– y, sobre todo, enunciada entre los principios –artículo 4.f) LAE– que han de inspirar la implantación y utilización de medios electrónicos por las Administraciones Públicas. De forma más precisa, el artículo 42 LAE se ha encargado de concretar su eficacia normativa al señalar que mediante una norma reglamentaria se aprobará el Esquema Nacional de Seguridad, donde han de establecerse los «principios básicos y requisitos mínimos que permitan una protección adecuada de la información».

¿Cuáles son, por tanto, esos requisitos mínimos cuya vulneración podría afectar a las actuaciones y comunicaciones que lleven a cabo las Administraciones Públicas utilizando medios electrónicos o, en su caso, determinar la exigencia de responsabilidades, ya patrimonial a la institución ya personal a las autoridades y el personal al servicio de la correspondiente Administración Pública? Al margen de la efectiva

implantación de, al menos las medidas de seguridad a que se refiere el artículo 27 ENS, y que, de manera precisa, se contemplan en el Anexo II, se han de cumplir ciertas obligaciones formales cuya inobservancia no supone necesariamente que no se hayan adoptado materialmente las precauciones correspondientes pero que, sin embargo, podrían ser un indicio de que no se satisfacen los estándares mínimos que contempla el propio Esquema. En primer lugar, se exige la aprobación formal de una política de seguridad en cada entidad, si bien en el ámbito municipal –artículo 11.2– podrá ser común para varios de ellos. En segundo lugar, para el análisis y el tratamiento de los riesgos de seguridad se ha de emplear una metodología reconocida internacionalmente –artículo 12–, no bastando por tanto acudir a fórmulas que ofrezcan un menor nivel de garantía, si bien a estos efectos deberá tenerse en cuenta el cumplimiento de la normativa administrativa aplicable en cada caso en función de la entidad de que se trate. Asimismo, con carácter previo a su instalación en el sistema, se requiere autorización expresa de cualquier elemento físico o lógico –artículo 20– a fin de constatar que cumple con las exigencias mínimas de seguridad. Por último, con la finalidad de asegurar el efectivo cumplimiento de las previsiones del Esquema, resulta preceptivo el registro de «las actividades de los usuarios, reteniendo la información necesaria para monitorizar, analizar, investigar y documentar actividades indebidas o no autorizadas, permitiendo identificar en cada momento a la persona que actúa».

Por lo que se refiere a la efectiva exigibilidad de tales medidas, con carácter general han de respetarse desde la entrada en vigor del ENS, es decir, son obligatorias desde comienzos del año 2011 si bien, excepcionalmente y siempre

que se hubiese aprobado un plan de adecuación, se podría demorar su efectiva aplicación dos años más. Fuera de estos supuestos, el incumplimiento de las previsiones del ENS podría afectar a las garantías técnicas que han de respetar los servicios de Administración electrónica y, en consecuencia, los derechos de los ciudadanos. Más allá de las implicaciones en orden a la responsabilidad patrimonial por los daños que se causen –que exige una relación de causalidad que no siempre se dará–, la principal deficiencia del marco normativo que en orden a la seguridad técnica prevé el Esquema es la ausencia de consecuencias expresas en su articulado para hacer frente a los supuestos de incumplimiento; lo que sin duda conlleva un riesgo inadmisible desde la perspectiva de la seguridad jurídica, dada la íntima relación que ya hemos destacado entre esta última y el cumplimiento de las normas técnicas en tanto que garantía de aquélla. Únicamente en el caso de los sistemas de categoría ALTA, a la vista del dictamen de auditoría, «el responsable del sistema podrá acordar la retirada de operación de alguna información, de algún servicio o del sistema en su totalidad, durante el tiempo que estime prudente y hasta la satisfacción de las modificaciones prescritas».

Es decir, salvo en este caso concreto, el ENS ha renunciado a concretar las consecuencias prácticas del incumplimiento de las garantías técnicas que establece, hasta el punto de que la anterior medida cautelar sólo se contempla para el supuesto de que, al menos, se hubiese realizado la auditoría que contempla el artículo 34; sin que por el contrario se prevean las implicaciones de una situación de claro y abierto menosprecio a sus previsiones, como sucedería en el caso de que ni siquiera se lleve a cabo la auditoría de seguridad que

exige el citado precepto. Esta insuficiencia sólo puede tener como explicación el temor a que se debieran paralizar aquellos servicios de Administración electrónica que no cumplan con las exigencias que se prevén en el Esquema, consecuencia que en todo caso resulta inadmisible desde la perspectiva jurídica. En efecto, las garantías de seguridad se encuentran fijadas normativamente y, por tanto, no es tolerable que su incumplimiento no tenga consecuencias jurídicas, ya que nos encontramos ante un principio con fundamento constitucional –artículo 18.4 CE–, consagrado legamente y cuyo alcance ha sido precisado reglamentariamente. Volveremos más adelante en el epígrafe III.2 sobre las consecuencias concretas que cabe derivar del incumplimiento del ENS.

Una reflexión final, no por ello menos importante, debe ser realizada. ¿Hasta qué punto las entidades locales se encuentran en muchos casos en disposición de cumplir estas exigencias de seguridad? Ciertamente, el planteamiento del ENS es adecuado para entidades administrativas dotadas de medios personales y materiales suficientes para satisfacer tales objetivos y, en ese sentido, la Administración General del Estado, las comunidades autónomas, diputaciones provinciales y grandes municipios deberían cumplir escrupulosamente sus exigencias, ¿pero qué sucede con el resto de Administraciones Públicas? Ciertamente, la obligación legal de que presten servicios electrónicos en función de sus disponibilidades presupuestarias cobra todo su sentido por lo que respecta a las exigencias del ENS, de manera que si no se encuentran en condiciones de asumirlas lo que procede es que las entidades de ámbito territorial superior antes referidas presten su apoyo a tal efecto. Así pues, resulta jurídicamente inadmisible que se presten servicios de Ad-

ministración electrónica sin cumplir escrupulosamente las exigencias normativas de seguridad ya que, de hacerse, se podría estar vulnerando la garantía del ciudadano consagrada en el artículo 18.4 CE en relación con el uso de la informática. En definitiva, aun a costa de limitar las posibilidades de modernización de la gestión, la innovación tecnológica debe descansar en el efectivo respeto de las exigencias jurídicas relativas a la seguridad.

b) Las condiciones de interoperabilidad y el ENI

Junto al ENS también se ha previsto legalmente la existencia de una normativa específica relativa a la interoperabilidad, concepto de carácter técnico que, no obstante y según contempla dicha regulación, también presenta implicaciones organizativas y semánticas que, en última instancia, resultan imprescindibles a la hora de plantear servicios basados en la innovación tecnológica; aun cuando dificulten su efectiva consecución en la medida que, como ha destacado Gamero, todas estas perspectivas complican especialmente dicho objetivo[116]. Más allá de las exigencias relativas a las comunicaciones con los ciudadanos que habrán de estar basadas en ciertos estándares definidos legalmente –en concreto *abiertos* así como, en su caso y de forma complementaria, aquéllos que sean de uso generalizado, según prevé el artículo 4.f) LAE–, el propio legislador establece la necesaria premisa de la interoperabilidad en muchas de sus previsiones. Esto sucede, por ejemplo, al referirse al principio de cooperación

[116] E. Gamero Casado, «Interoperabilidad y Administración electrónica: conéctense, por favor», *Revista de Administración Pública*, núm. 179, 2009, pp. 292 y ss., donde no obstante se destaca su carácter de «piedra angular para el impulso de la administración electrónica integral».

–artículo 4.e–, a la configuración de las sedes electrónicas –artículo 10.3–, las condiciones en que resultarán admisibles los certificados de firma electrónica –artículo 21– o la aportación de documentos a través de los registros electrónicos –artículo 25–, al margen de la regulación específica del Título IV en su Capítulo II bajo el prisma de la cooperación interadministrativa[117].

Estas genéricas previsiones han sido concretadas a través del ENI que, al igual que sucede en el ámbito de la seguridad, ha adoptado la forma de una disposición de carácter reglamentario ya que su aprobación ha tenido lugar a través de un Real Decreto cuyo ámbito de aplicación coincide con el de la propia Ley, de manera que su contenido tiene igualmente carácter básico y, por tanto, es de aplicación en todas las Administraciones Públicas. Sin embargo, la regulación del ENI ha sido objeto de concreción a través de numerosas *normas técnicas* dictadas al amparo de su disposición adicional primera, que han sido aprobadas mediante resoluciones de altos cargos estatales y que, no obstante, también son de obligado cumplimiento por parte de todas las Administraciones Públicas al igual que el ENI.

Ahora bien, dicha vinculación ha de ser matizada por cuanto, a pesar de que formalmente se ha facilitado la participación de tales entidades en el procedimiento de elaboración

---

[117] En relación con las diferentes modalidades que puede revestir este principio por lo que se refiere a la cuestión abordada desde el punto de vista de algunas experiencias prácticas, veáse A. Cerrillo i Martínez, «Cooperación entre Administraciones Públicas para el impulso de la Administración electrónica», en E. Gamero Casado y J. Valero Torrijos (coords.), *La Ley de Administración electrónica. Comentario sistemático a la Ley 11/2007, de 22 de junio, de Acceso Electrónico de los Ciudadanos a los Servicios Públicos*, 3ª ed., Thomson-Aranzadi, Madrid, 2010, pp. 775 a 780.

del ENI, no es admisible que a través de las referidas normas técnicas –que, además, son actos administrativos y no tienen carácter normativo– se pueda llegar al extremo de imponer concretas decisiones que vulneren la autonomía organizativa constitucionalmente garantizada a las comunidades autónomas y entidades locales territoriales, tal y como podría considerarse, por ejemplo, con la fijación de una calidad mínima en las imágenes digitalizadas. Más allá de la valoración que merezcan estas soluciones desde la perspectiva constitucional y, en concreto, el alcance de la intervención estatal en la fijación de las bases del régimen jurídico de las Administraciones Públicas, nos encontramos ante una exigencia técnica –la interoperabilidad– que plantea una clara centralización competencial en manos de la Administración General del Estado que, para resultar admisible, ha de permitir al resto de entidades ejercer razonablemente sus propias competencias organizativas. Y, por otra parte, la exigencia de garantizar la interoperabilidad obliga a reforzar los mecanismos de cooperación y coordinación, de manera que se facilite tanto el ejercicio de los derechos de los interesados como, sobre todo, la actividad administrativa que permita ofrecer servicios avanzados basados en el intercambio documental. Volveremos sobre esta problemática en el capítulo siguiente al analizar la perspectiva jurídica de la interoperabilidad en relación con los documentos electrónicos.

Al igual que sucedía en materia de seguridad, el ENI no ha establecido con rotundidad las consecuencias jurídicas de su incumplimiento[118], más allá de la prohibición de adquirir

[118] Aun cuando E. Gamero Casado haya mantenido que el ENI apuesta por un «modelo de interoperabilidad vinculante, rígido y centralizado» («In-

sistemas que no se diseñen conforme a sus exigencias[119] –artículo 5 ENI–, lo que nos lleva a ampliar la necesidad de su respeto también a los casos en que el desarrollo de los sistemas se hubiere realizado por el personal de la propia entidad. Todo ello con idéntico horizonte temporal que en el caso del ENS, cuyas previsiones en cuanto a la entrada en vigor son similares salvo un matiz relevante: la exigibilidad de las normas de interoperabilidad se condiciona en los términos de la disposición final tercera LAE, de manera que podría quedar diferida en los ámbitos autonómicos y local, en relación con ciertas actuaciones y procedimientos para los cuales no existiesen suficientes disponibilidades presupuestarias; circunstancia cuya valoración, tal y como antes advertíamos, ha de tener en cuenta el coste necesario para implementar efectivamente las normas de seguridad.

Sin embargo, a diferencia de lo que sucede en el ámbito de la seguridad, las consecuencias del incumplimiento de las exigencias de interoperabilidad van más allá simplemente de la puesta en riesgo de la información o el funcionamiento de los sistemas y aplicaciones, ya que esconden un riesgo menos

---

teroperabilidad y Administración electrónica…», ob. cit., p. 328), lo cierto es que se ve obligado a reconocer igualmente el riesgo de bloqueo en el ámbito institucional por lo que se refiere a sus herramientas de desarrollo (ibídem, p. 331). En última instancia, no se trata únicamente ya de la falta de exigibilidad de los derechos al uso de medios electrónicos en la totalidad de los trámites y procedimientos en relación con las Administraciones autonómicas y locales sino, específicamente en relación con la interoperabilidad, de la ausencia de mecanismos que aseguren que los servicios ofrecidos respeten las exigencias previstas en el ENI.

[119] No obstante, CERRILLO incluye entre las garantías de cumplimiento de las exigencias del ENI otros mecanismos adicionales como las disposiciones de creación de las sedes y los registros electrónicos (A. CERRILLO I MARTÍNEZ, «Cooperación entre Administraciones…», ob. cit., p. 792).

visible pero devastador para la confianza de los ciudadanos y, en última instancia, el efectivo respeto de sus derechos, el correcto funcionamiento de los servicios según las previsiones legales o, sin ánimo exhaustivo, la accesibilidad de la información.

Por lo que respecta al derecho a no presentar documentos que ya obren en poder de las Administraciones Públicas o, simplemente, el intercambio documental entre entidades distintas, los inventarios que contempla el artículo 9 ENI resultan esenciales, si bien no se prevén consecuencias concretas para las Administraciones que incumplan esta obligación, perjudicándose de esta manera tanto a los intereses públicos en juego como a la posición jurídica de los ciudadanos. Más grave resulta, incluso, el supuesto en que como consecuencia del incumplimiento de los estándares fijados se impida el ejercicio de derechos o el cumplimiento de obligaciones relacionadas con la presentación o recepción de comunicaciones; si bien en este caso cabría entender que cuando no se hubiesen respetado las condiciones del artículo 11.2 ENI sería inadmisible admitir la utilización de un estándar no abierto para dichas comunicaciones, al menos en la medida que se perjudique ilícitamente al ciudadano.

Más allá de que se pudiera dejar sin efecto el derecho de acceso a los archivos y registros administrativos, el incumplimiento de los criterios de interoperabilidad en la conservación de los documentos y los expedientes electrónicos con vistas a su posterior recuperación –artículos 21 y 23 ENI– podría suponer un serio perjuicio para los intereses públicos vinculados, hasta el punto de que cabría dudar de la eficacia de los documentos –o, incluso, de su validez en

la medida que suponga una vulneración de los derechos de los ciudadanos– en aquellos casos en que no fuese factible acceder a los mismos. Salvo, claro está, que la infracción condicione la integridad de la información, en cuyo caso podría verse afectada incluso la validez de los documentos generados sin respetar las condiciones generales exigidas por el artículo 45.4 LRJAP; problemática de la que nos ocuparemos detenidamente en el epígrafe III.2.

Así pues, las garantías de interoperabilidad constituyen un desafío para el diseño y la ejecución de los proyectos de Administración electrónica si se pretenden superar los problemas, inconvenientes y disfuncionalidades de la Administración basada en el uso del papel y las relaciones presenciales. Sin embargo, la modernización tecnológica se está llevando a cabo en muchos casos sin tener en cuenta suficientemente las exigencias que conlleva este principio, de manera que la seguridad jurídica se puede ver seriamente afectada, al margen de otras negativas consecuencias más allá del Derecho como la falta de confianza de los ciudadanos al percibir que, a pesar de los importantes esfuerzos presupuestarios realizados, no mejoran sustancialmente ni la eficacia y la eficiencia de la Administración Pública ni las condiciones en que ejercen sus derechos y cumplen sus obligaciones.

III. ENTRE EL CUMPLIMIENTO DEL DERECHO Y EL POTENCIAL INNOVADOR DE LA ADMINISTRACIÓN ELECTRÓNICA: PERSPECTIVA JURÍDICA DE UN DIFÍCIL EQUILIBRIO

1. LA NECESARIA RECONFIGURACIÓN DE LOS CONCEPTOS JURÍDICOS AL TRASLUZ DE LAS SINGULARIDADES TECNOLÓGICAS

Una de las principales manifestaciones de las tensiones entre las normas jurídicas y la tecnología se refiere a la necesidad de que los conceptos en los que tradicionalmente se ha basado el Derecho sean adaptados a las singularidades que plantea esta última ya que, de lo contrario, podrían dejar de cumplir la función que originariamente satisfacían. Más aún, como analizaremos más adelante, la obsolescencia en los conceptos y categorías jurídicas podría afectar negativamente a las garantías establecidas normativamente, generando una apariencia de protección que, sin embargo, puede resultar incluso contraproducente debido a su desfase. Ahora bien, no se trata de sustituir las bases conceptuales a partir de las cuales se articula el régimen jurídico de las Administraciones Públicas sino, por el contrario, de reformular su alcance cuando resulte preciso, todo ello con el objetivo de lograr una mejor adaptación a la realidad tecnológica sobre la que se proyecta.

Desde estos planteamientos, el principio de competencia en relación con la innovación tecnológica en la gestión administrativa adquiere un nuevo significado, tal y como ya se adelantase en el capítulo anterior. En efecto, en la concepción tradicional de la persona jurídico-administrativa

el concepto de los órganos se ha construido a partir de su consideración como parte de la estructura organizativa de la Administración Pública a la que se le atribuyen ciertas competencias en tanto que parcelas del poder público. Al frente de los órganos se encuentran las personas físicas a las que corresponde su titularidad, ya sean unipersonales o colegiados, de manera que son dichas personas las que proceden a adoptar decisiones en el ejercicio de las correlativas competencias asignadas. Sin embargo, el uso de medios electrónicos en la adopción de decisiones puede alterar las premisas conceptuales antes referidas, en particular cuando se pretenda su plena automatización, ya que en los supuestos en que se acuda a la informática como una herramienta de apoyo a la decisión de los titulares de los órganos existirá, al menos, una vinculación formal entre estos últimos y el ejercicio competencial.

Por el contrario, la actuación automatizada implica que dichos titulares ni siquiera participan indirectamente en la formación de la decisión administrativa que, en consecuencia, se adopta a partir del funcionamiento de aplicaciones informáticas que han sido diseñadas por el personal técnico al servicio de la Administración Pública o, incluso, por la correspondiente entidad privada que hubiese sido seleccionada previo el correspondiente procedimiento contractual. En consecuencia, sólo acudiendo a una ficción legal cabe considerar que la actuación se ha llevado a cabo por el órgano que tenía atribuida la competencia que, a lo sumo, podría haber emitido un informe en relación con el funcionamiento de una aplicación informática que, debido a la complejidad que conlleva, con relativa frecuencia ni siquie-

ra podría comprender y mucho menos controlar[120]. Parece pues más que justificado que la actuación de que se trate se entienda atribuida no ya a un órgano en concreto, y menos aún a su titular, sino antes bien a la entidad considerada como persona jurídica, de manera que nos encontraríamos en realidad ante una imputación institucional que supera los contornos conceptuales de la teoría del órgano en la que tradicionalmente se había asentado, incluso, la validez de los actos administrativos.

Más aún, en estos casos cabría poner en duda que nos encontremos ante auténticos actos administrativos en el sentido de que hayan sido dictados por el órgano competente a través de su titular ya que, como se ha razonado con anterioridad, su participación sería a lo sumo meramente formal. Así pues, este tipo de supuestos han de reconducirse a la categoría de actuaciones administrativas ya que, de lo contrario, se corre el riesgo de seguir utilizando un concepto dotado de unos elementos cuya efectiva presencia en este tipo de supuesto simplemente no se daría y, por tanto, cuya validez en términos jurídicos ha de ser al menos discutida. En consecuencia, las garantías jurídicas a partir de las cuales se fundamenta la actuación administrativa también deben rediseñarse a fin de garantizar, al menos, el efectivo control no ya por las personas físicas titulares de los órganos sino,

---

[120] Por ello cobra especial trascendencia el estricto cumplimiento de las exigencias en orden a la concreción expresa de las razones que avalan la posibilidad de automatizar el proceso decisor (I. Martín Delgado, «Naturaleza…», ob. cit. p. 373); premisa que se ha llegado a formular genéricamente en la necesidad de que conlleve una mejora de la eficiencia administrativa (I. Alamillo Domingo y X. Uríos Aparisi, *La actuación administrativa automatizada…*», ob. cit., p. 18).

al menos, por la entidad en su conjunto, tal y como sucede con las herramientas utilizadas para asegurar la integridad y autenticidad de la actuación automatizada.

De la misma manera, el concepto de firma como instrumento mediante el que una persona física dota de autenticidad a un documento y a través del cual expresa que aprueba su contenido resulta claramente insuficiente, al menos en ciertos casos, cuando se proyecta sobre el uso de medios electrónicos en la actividad administrativa. En efecto, en primer lugar la firma electrónica plantea la importante singularidad de que la persona física no tiene una intervención directa e inescindible cuando la utiliza, de manera que su identidad podría ser suplantada por un tercero cuando disponga de acceso a la clave privada y tenga la información necesaria –es decir, caso de la contraseña si estuviese habilitada–: de darse estas premisas, podría utilizar la firma electrónica de otro sujeto sin que, salvo que concurran circunstancias adicionales, pueda detectarse que ha habido un uso indebido de esta herramienta de identificación y autenticación. En consecuencia, a la hora de afrontar eventuales problemas relacionados con este asunto debería tenerse en cuenta que más que de una firma se trata de un sello, en el sentido de que no se puede garantizar más que a través de una ficción legal que quien generó la firma electrónica fuese directa y personalmente el titular del certificado.

Precisamente, teniendo en cuenta esta premisa y, sobre todo, la falta de actuación de personas físicas, la legislación sobre Administración electrónica ha creado dos mecanismos de autenticación que, al contrario de lo que sucede con la regulación general en materia de *firma* electrónica, no utilizan

dicho sustantivo[121]: son los denominados sello de órgano y sello de entidad. En efecto, se trata de instrumentos que no se vinculan directamente a personas físicas, de manera que su utilización se reserva legalmente para aquellos supuestos en que se lleven a cabo actuaciones automatizadas, debiéndose acudir a uno u otro según que las mismas se encuentren reservadas a un órgano concreto en función de la correspondiente asignación competencial o, por el contrario, no se haya precisado dicha exigencia y, por tanto, se considere que la actuación se lleva a cabo en abstracto por la entidad.

Sin embargo, la identificación de las personas jurídicas cuando realizan trámites por medios electrónicos ha tenido por el contrario una respuesta normativa que al menos habría que considerar confusa en el ámbito general y, en particular, a efectos tributarios; planteamiento que demuestra claramente la necesidad de adaptación conceptual a la que nos estamos refiriendo. En concreto, se admite la denominada firma de personas jurídicas para hacer referencia, en realidad, a un supuesto de representación de estas últimas a través de personas físicas que llevan a cabo un trámite en su nombre. Es un contrasentido utilizar el concepto de firma en relación con las personas jurídicas ya que, como destacábamos anteriormente, únicamente puede relacionarse con las personas físicas y, aun cuando en estos casos se produzca su participación directa, la actuación se considera en última instancia realizada por la

[121] En todo caso, desde el punto de vista conceptual, debe advertirse que difícilmente cabe considerar a estos instrumentos como una firma electrónica ya que, tal y como han destacado I. Alamillo Domingo y X. Uríos Aparisi, sencillamente son instituciones nuevas y diferentes de la firma («El nuevo régimen legal…», ob. cit., p. 676).

entidad a los efectos jurídicos. Ciertamente, la vinculación permanente con una concreta persona física simplifica la gestión de identidades y la imputación de las actuaciones que se realicen, pero en puridad más que de un supuesto de firma electrónica de personas jurídicas nos encontramos ante un ejemplo de representación y, por tanto, debería ser tratado como tal no sólo a los efectos del régimen jurídico aplicable –en particular por lo que se refiere al alcance de la representación y el tipo de trámites que pueden realizarse– sino también del concepto utilizado, evitando de este modo confusiones innecesarias.

Por último, en relación con la perspectiva analizada en este epígrafe, es necesario enfatizar que la tecnología obliga a que el Derecho acoja y modele ciertos conceptos que, de este modo, adquieren una nueva dimensión que ha de ser tenida en cuenta necesariamente. Así sucede, por ejemplo, con la seguridad y, sobre todo, la interoperabilidad: el significado de estas expresiones no puede mantenerse intacto cuando se analizan desde el prisma jurídico a pesar de que el fundamento de las mismas siga siendo en gran medida tecnológico. En el caso de la interoperabilidad este planteamiento es sin duda más evidente por cuanto incluso la propia normativa se ha visto obligada a asumir su carácter poliédrico: en concreto, el ENI reconoce que habrá de tenerse en cuenta una triple perspectiva que, como analizamos anteriormente, englobaría no sólo la tecnológica en sí misma considerada sino, además, la semántica y la organizativa. Más aún, por lo que se refiere a esta última, su proyección jurídica y, en particular normativa, es más que evidente en algunos casos, tal y como sucede, por ejemplo, en relación con los requisitos establecidos en cada Administración Pública relativos al contenido y

los requisitos de los concretos documentos; de manera que, si no se produce previamente una normalización en cuanto a la regulación donde se contemplen, podría impedirse –o, al menos, dificultarse gravemente– la funcionalidad propia y característica de la interoperabilidad concebida como premisa para el normal funcionamiento de los servicios de Administración electrónica, en particular desde la perspectiva innovadora que requiere un modelo de gestión documental avanzado.

2. CONSECUENCIAS JURÍDICAS DEL INCUMPLIMIENTO DE LAS GARANTÍAS TECNOLÓGICAS

Aun cuando la tecnología puede ofrecer, en principio, mayores garantías que las actuaciones llevadas a cabo presencialmente, lo cierto es que tal premisa requiere que se apliquen efectivamente las oportunas medidas técnicas ya que, en caso de no hacerse, las consecuencias son ciertamente inevitables: se crea una apariencia formal de seguridad que en la práctica no se da y, por tanto, las posibilidades de accesos, alteraciones y manipulaciones indebidas se incrementan exponencialmente, afectando negativa e intensamente incluso a la validez jurídica de aquéllas; al margen, claro está, de otro tipo de consecuencias como la eventual responsabilidad que pueda derivarse o la desconfianza en la tecnología que puede generarse. Más aún, en muchos casos las propias Administraciones Públicas no adoptan las medidas técnicas necesarias para dar cumplimiento a las exigencias jurídicas, de manera que se implantan proyectos de modernización e innovación tecnológica en los que el grado de cumplimiento

de las disposiciones normativas que las contemplan es más que deficiente.

Ante la constatación de esta evidencia surge la necesidad de plantear las consecuencias jurídicas que conlleva el incumplimiento de las garantías tecnológicas fijadas normativamente por lo que respecta específicamente a las disposiciones reguladoras de la Administración electrónica. Primeramente debe recordarse que el artículo 18.4 de la Constitución establece como garantía al máximo nivel –el propio de los derechos fundamentales y libertades públicas incardinados en el Capítulo II del Título II– la limitación del «uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos». Si bien el Tribunal Constitucional ha llevado a cabo una injustificada interpretación restrictiva del alcance de este precepto al circunscribirlo al ámbito de la protección de los datos de carácter personal, tal y como ya justificó anteriormente, nada obsta para que dicha garantía se aplique también a los efectos de prohibir el uso de los medios electrónicos que vulnere las normas relativas a la seguridad tecnológica, al menos siempre que se impida el pleno ejercicio de los derechos de los ciudadanos. A este respecto debe tenerse en cuenta que las normas de seguridad han sido concretadas a nivel reglamentario a través del ENS, de manera que disponemos de los estándares tecnológicos a partir de los cuales poder evaluar la conformidad de las actuaciones administrativas desde la perspectiva que ahora nos ocupa.

Más allá del plano constitucional y de la tutela preferente y sumaria que se deriva de la ubicación sistemática del citado precepto, ante el silencio por parte del legisla-

dor que no ha establecido una previsión expresa al respecto, resulta imprescindible extraer por vía interpretativa las consecuencias que pueden derivarse del incumplimiento de las normas técnicas relativas a la seguridad de los servicios de Administración electrónica. Así, en primer lugar debe tenerse en cuenta que la vulneración de un derecho fundamental podría dar lugar a la nulidad de pleno derecho de los actos administrativos –artículo 62.1.a) LRJAP–, de manera que incurrirían en ella aquéllos que se hubiesen dictado sin respetar las reglas de seguridad esenciales que resulten de aplicación directa según las previsiones del ENS; al menos cuando como consecuencia de la infracción se impida el pleno ejercicio de sus derechos a los ciudadanos, tal y como exige la garantía constitucional[122]. De la misma manera, podría concluirse que la infracción de las reglas del ENI, en particular cuando supongan la utilización de estándares tecnológicos que incumplan los principios jurídicos en la materia, podrían determinar la nulidad de aquellas actuaciones administrativas que impidan a los ciudadanos el ejercicios de sus derechos legalmente reconocidos o, en su caso, el acceso a la información y los documentos a los que tengan derecho.

Esta misma consecuencia –la nulidad radical– se daría en el supuesto en que la infracción conlleve la vulneración manifiesta de las reglas de competencia por razón de la materia, problemática en relación con la cual las actuaciones automatizadas ofrecen una especial trascendencia. En

[122] Cfr., en sentido contrario, J. M. Molina Mateos, «Esquema Nacional de Seguridad», *Revista Aranzadi de Derecho y Nuevas Tecnologías*, núm. 23, 2010, p. 62.

efecto, podría darse el caso de que las reglas competenciales hayan reservado a un determinado órgano administrativo una concreta actuación de manera que, mientras permanezcan vigentes, será precisa al menos la intervención formal de aquél a través del correspondiente sello de órgano; en consecuencia, no serviría otro instrumento para asegurar el cumplimiento de los requerimientos legales de integridad y autenticidad. Más aún, también habrían de respetarse las exigencias esenciales que, desde el punto de vista sustantivo, se hayan fijado para las actuaciones automatizadas, en particular las que se refieren a las condiciones técnicas para su correcto funcionamiento[123]. En el resto de casos que no puedan considerarse meros defectos de forma, el incumplimiento de las normas relativas a la seguridad tecnológica habrá de reconducirse a la anulabilidad, es decir, siempre que se trate de infracciones que no impidan el ejercicio de los derechos a los interesados y no encajen en los supuestos de nulidad absoluta.

En todo caso, además de tales requisitos, con carácter general es necesario que el incumplimiento de las medi-

[123] En concreto, por lo que respecta a la Administración General del Estado, el artículo 39 LAE requiere que se establezcan previamente «el órgano u órganos competentes, según los casos, para la definición de las especificaciones, programación, mantenimiento, supervisión y control de calidad y, en su caso, auditoría del sistema de información y de su código fuente». Sin embargo, este precepto carece de naturaleza básica y, por tanto, su aplicación en otros ámbitos distinto de aquél quedaría desplazada por las previsiones de la correspondiente normativa aplicable, más allá de su efectividad como regla supletoria. Por el contrario, los incumplimientos meramente formales deberían ser reconducidos a la anulabilidad, tal y como sucedería, por ejemplo, con la exigencia relativa a la indicación del órgano responsable de la actuación a los efectos de la competencia judicial para su eventual impugnación que establece ese mismo precepto.

das de seguridad y la causa de invalidez –ya sea nulidad, ya sea anulabilidad– tengan una relación directa que justifique el alcance de tales consecuencias: no bastaría, por tanto, la simple concurrencia de circunstancias genéricas como el mero hecho de no haber implantado las medidas de seguridad previstas en cada caso según el tipo de servicio o el trámite de que se trate. En estos casos, por el contrario, aunque no pueda afirmarse la invalidez de la actuación realizada, sí que se debería adoptar de oficio –y, por supuesto, a solicitud del interesado– la medida cautelar que consiste en la paralización del funcionamiento de los servicios afectados hasta que no se satisfagan las garantías técnicas previstas en la normativa que, en cada caso, resulte de aplicación[124].

Una consecuencia adicional podría derivarse del incumplimiento de las normas de seguridad exigibles y, en particular, de las previstas en el ENS, por lo que respecta a la presunción de validez de los actos administrativos que declara el artículo 57 LRJAP. En concreto, esta singular eficacia parte de la premisa del cumplimiento de las normas jurídicas que resulten de aplicación a los actos administrativos de que se traten, exigencia que también afecta a las anteriormente referidas[125]. Así pues, en el supuesto de que el interesado alegue y demuestre el incumplimiento de las previsiones del

---

[124] Precisamente, se trata de la consecuencia prevista de manera expresa en materia de protección de datos personales por el artículo 49 LOPD para los «supuestos constitutivos de infracción grave o muy grave en que la persistencia en el tratamiento de los datos de carácter personal o su comunicación o transferencia internacional posterior pudiera suponer un grave menoscabo de los derechos fundamentales de los afectados».

[125] En relación con esta idea, cfr. J. M. Molina Mateos, «Esquema Nacional de Seguridad», ob. cit., p. 62.

ENS y la afectación a su posición jurídica como destinatario del acto en cuestión cabría afirmar que dicha presunción quedaría destruida y, en consecuencia, sería la propia Administración la que, ante la oposición del ciudadano, debería demostrar que a pesar del incumplimiento el acto afectado respeta las exigencias y garantías técnicas necesarias para desplegar sus efectos sin causar perjuicios al interesado. Este sería, pues el sentido, de la previsión del artículo 31 ENS al afirmar, en relación con las comunicaciones, que cuando sean realizadas en los términos fijados por el propio Esquema, «tendrán el valor y la eficacia jurídica que corresponda a su respectiva naturaleza, de conformidad con la legislación que resulte de aplicación»; de modo que si no se respetasen tales condiciones la conclusión sería, *sensu contrario*, la imposibilidad de que las comunicaciones desplieguen sus plenos efectos ante una eventual impugnación por parte de los destinatarios.